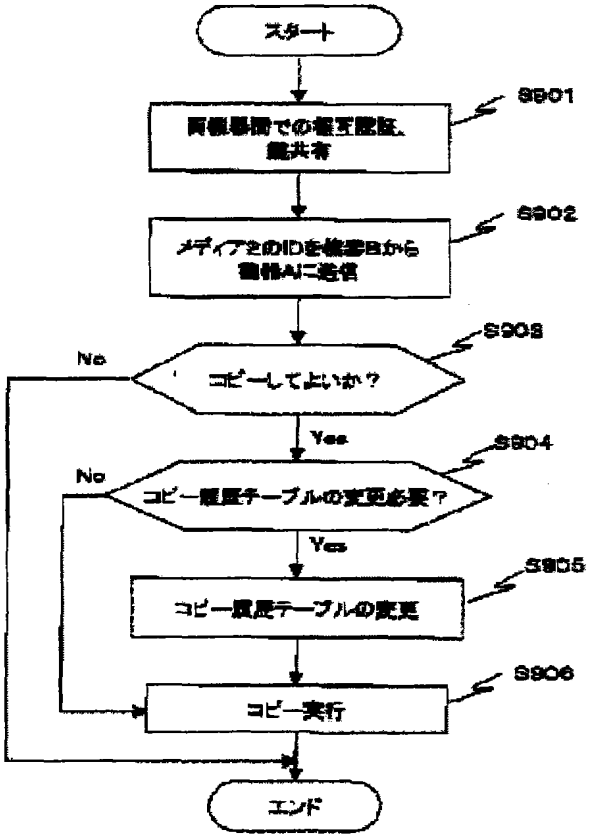
INFORMATION PROCESSOR, INFORMATION PROCESSING METHOD, INFORMATION RECORDING MEDIUM AND PROGRAM PROVIDING MEDIUM

Publication number: JP2001351322
Publication date: 2001-12-21
Inventor: ASANO TOMOYUKI; OSAWA YOSHITOMO; NAKANO KATSUHIKO; KITAJIMA MARIKO
Applicant: SONY CORP
Classification:
- international: ***G06F12/14; G06F21/24; G06Q50/00; G11B20/10;*** **G06F12/14; G06F21/00; G06Q50/00; G11B20/10;** (IPC1-7): G11B20/10; G06F12/14; G06F17/60
- European:
Application number: JP20000170603 20000607
Priority number(s): JP20000170603 20000607

Abstract of **JP2001351322**

PROBLEM TO BE SOLVED: To provide an information processor and an information processing method which can limit the number of copies. SOLUTION: This constitution includes a copy history table where the number of allowable copies is set in response to the contents data in addition to the contents. The copy history table is prepared for every content data. On the basis of the tables, it is decided whether or not the copy processing should be carried out. Then the copy processing is inhibited after number of copies reaches the upper limit. The IDs of media which carry out the copy processing are written in a copy storage destination media ID column set in response to the contents IDs in the copy history tables before the copy processing carried out to another device. When the number of copies exceeds the number set as the copy numbers of the copy history tables, the media IDs are not written and the copy processing is not permitted.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－351322
（P2001－351322A）
(43)公開日　平成13年12月21日(2001.12.21)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	５Ｂ０１７
			Ｄ	５Ｂ０４９
			Ｆ	５Ｄ０４４
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｅ	
			３２０Ｆ	

審査請求　未請求　請求項の数25　ＯＬ　（全 25 頁）　最終頁に続く

(21)出願番号　特願2000－170603(P2000－170603)

(22)出願日　平成12年６月７日(2000.6.7)

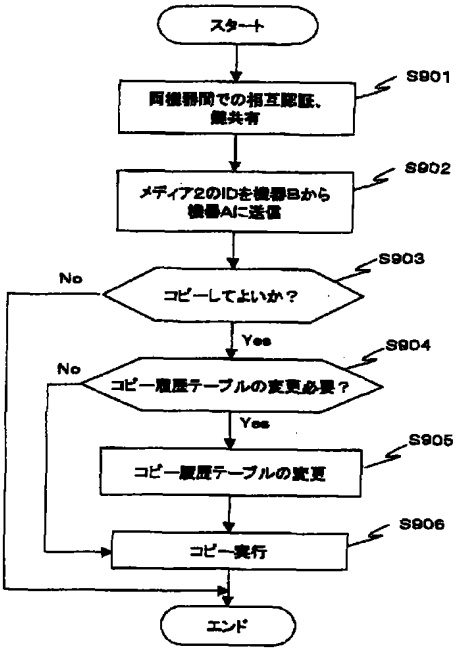
特許法第64条第２項ただし書の規定により×印の部分は不掲載とした。

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　浅野　智之
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　大澤　義知
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100101801
弁理士　山田　英治　（外２名）

最終頁に続く

(54)【発明の名称】　情報処理装置、情報処理方法、および情報記録媒体、並びにプログラム提供媒体

(57)【要約】
【課題】　コピーの数を制限することを可能とした情報処理装置および情報処理方法を提供する。
【解決手段】　コンテンツデータに対応して許容可能なコピー数を設定したコピー履歴テーブルをコンテンツとともに保有する構成とした。コンテンツデータごとにコピーの履歴テーブルを作成し、それに基づいてコピーを行うかどうか判定し、上限に達した以降のコピー処理を不可とする。他デバイスに対するコピー実行の前に、コピー履歴テーブル中のコンテンツＩＤに対応して設定されたコピー格納先メディアＩＤ欄に、コピーを実行するメディアのメディアＩＤを書き込む処理を実行する構成とし、コピー履歴テーブルのコピー番号として設定された数を超える場合は、メディアＩＤの書き込みが実行されずコピーを不許可とする。



1

【特許請求の範囲】

【請求項１】コンテンツデータを格納したコンテンツ格納記録媒体からコンテンツデータを他の情報処理装置または他の記録媒体に出力可能な情報処理装置において、前記コンテンツ格納記録媒体に格納されたコンテンツデータについての、前記他の情報処理装置または他の記録媒体に対するコピー可否判定処理を、前記コンテンツデータ毎のコピー可能回数を設定したコピー履歴テーブルに基づいて判定する制御手段を有することを特徴とする情報処理装置。

【請求項２】前記コピー履歴テーブルには、コピー可能回数に対応して設定されるコピー番号と、コピー番号毎に対応して設定されるコピー格納先メディアＩＤ設定欄を有し、

前記制御手段は、

コンテンツデータのコピー先となる他の情報処理装置または他の記録媒体の識別子を前記コピー格納先メディアＩＤ欄に記録したことを条件として前記コンテンツ格納記録媒体からのコピーを実行する構成を有することを特徴とする請求項１に記載の情報処理装置。

【請求項３】前記コピー履歴テーブルは、

前記コンテンツ格納記録媒体、または該コンテンツ格納記録媒体を装着した情報処理装置内のメモリに暗号化されたデータとして格納された構成であることを特徴とする請求項１に記載の情報処理装置。

【請求項４】前記コピー履歴テーブルの暗号化キーは、前記コンテンツ格納記録媒体の識別子と、前記情報処理装置に格納されたマスターキーとに基づいて生成される暗号化キーであることを特徴とする請求項３に記載の情報処理装置。

【請求項５】前記コピー履歴テーブルには、コピー可能回数に対応して設定されるコピー番号と、コピー番号毎に対応して設定されるコピー格納先メディアＩＤ設定欄を有し、

前記制御手段は、

コンテンツデータのコピー先となる他の情報処理装置または他の記録媒体の識別子と同一の識別子が既に前記コピー格納先メディアＩＤ欄に記録されている場合には、同一の識別子を有する他の情報処理装置または他の記録媒体に対する前記コンテンツ格納記録媒体からのコピーを実行する構成を有することを特徴とする請求項１に記載の情報処理装置。

【請求項６】前記コピー履歴テーブルには、複数のコンテンツデータの各々に対応して許容可能な個別のコピー可能回数が設定された構成であることを特徴とする請求項１に記載の情報処理装置。

【請求項７】前記情報処理装置は、さらに、

コピーの可否を設定したコピー制御情報に基づいて、前記コンテンツデータを格納したコンテンツ格納記録媒体からのコンテンツデータのコピーの可否を判定する構成を有し、

2

前記コピー制御情報には、コピーの可否とともに、コピーの許容回数が設定されていることを示す態様としての、コピー数制限ありを示す情報を含み、

前記制御手段は、

前記コピー制御情報がコピー数制限ありを示す情報であるか否かを判定し、コピー数制限ありを示すコピー制御情報であると判定されたことを条件として、前記他の情報処理装置または他の記録媒体に対するコピー可否判定処理を、前記コンテンツデータ毎のコピー可能回数を設定したコピー履歴テーブルに基づいて実行する構成を有することを特徴とする請求項１に記載の情報処理装置。

【請求項８】前記情報処理装置は、さらに、

コンテンツデータの受信に際して、コピーの可否を設定したコピー制御情報を受信し、コピー制御情報が、コピーの許容回数が設定されていることを示す態様としてのコピー数制限ありを示す情報である場合に、前記コピー履歴テーブルを生成して、生成したコピー履歴テーブルに基づくコピー制御処理を実行する構成を有することを特徴とする請求項１に記載の情報処理装置。

【請求項９】前記情報処理装置は、さらに、

コンテンツデータの受信に際して、コピーの可否を設定したコピー制御情報を受信し、コピー制御情報が、コピーの許容回数が設定されていることを示す態様としてのコピー数制限ありを示す情報であり、さらにコピーの許容回数の指定データが前記コピー制御情報中に含まれる場合に、前記コピー履歴テーブルを、前記コピー制御情報中のコピーの許容回数データに基づいて生成して、生成したコピー履歴テーブルに基づくコピー制御処理を実行する構成を有することを特徴とする請求項８に記載の情報処理装置。

【請求項１０】前記情報処理装置は、さらに、

コンテンツデータの受信に際して、コピーの可否を設定したコピー制御情報を受信し、コピー制御情報が、コピーの許容回数が設定されていることを示す態様としてのコピー数制限ありを示す情報であり、コピーの許容回数の指定データが前記コピー制御情報中に含まれない場合に、前記コピー履歴テーブルを、前記情報処理装置に予め設定済みのコピー許容回数データに基づいて生成して、生成したコピー履歴テーブルに基づくコピー制御処理を実行する構成を有することを特徴とする請求項８に記載の情報処理装置。

【請求項１１】前記情報処理装置は、さらに、

コンテンツデータの受信に際して、受信コンテンツに対応するコピー履歴テーブルを受信し、受信したコピー履歴テーブルに基づくコピー制御処理を実行する構成を有することを特徴とする請求項１に記載の情報処理装置。

【請求項１２】コンテンツデータを格納したコンテンツ格納記録媒体からコンテンツデータを他の情報処理装置または他の記録媒体に出力可能な情報処理装置における

情報処理方法であり、
前記コンテンツ格納記録媒体に格納されたコンテンツデータについての、前記他の情報処理装置または他の記録媒体に対するコピー可否判定処理を、前記コンテンツデータ毎のコピー可能回数を設定したコピー履歴テーブルに基づいて判定することを特徴とする情報処理方法。
【請求項１３】前記コピー履歴テーブルには、コピー可能回数に対応して設定されるコピー番号と、コピー番号毎に対応して設定されるコピー格納先メディアＩＤ設定欄を有し、
前記コピー可否判定処理は、
コンテンツデータのコピー先となる他の情報処理装置または他の記録媒体の識別子を前記コピー格納先メディアＩＤ欄に記録可能か否かを判定するステップと、
前記コピー格納先メディアＩＤ欄に記録可能であることを条件として前記コンテンツ格納記録媒体からのコピーを可能と判定するステップと、
を含むことを特徴とする請求項１２に記載の情報処理方法。
【請求項１４】前記情報処理方法において、さらに、
前記コンテンツ格納記録媒体の識別子と、前記情報処理装置に格納されたマスターキーとに基づいて、暗号化キーを生成し、
前記暗号化キーに基づいて前記コピー履歴テーブルを暗号化して前記コンテンツ格納記録媒体、または該コンテンツ格納記録媒体を装着した情報処理装置内のメモリに格納する処理を実行することを特徴とする請求項１２に記載の情報処理方法。
【請求項１５】前記コピー履歴テーブルには、コピー可能回数に対応して設定されるコピー番号と、コピー番号毎に対応して設定されるコピー格納先メディアＩＤ設定欄を有し、
前記コピー可否判定処理は、
コンテンツデータのコピー先となる他の情報処理装置または他の記録媒体の識別子と同一の識別子が既に前記コピー格納先メディアＩＤ欄に記録されている場合には、同一の識別子を有する他の情報処理装置または他の記録媒体に対する前記コンテンツ格納記録媒体からのコピーを実行可と判定することを特徴とする請求項１２に記載の情報処理方法。
【請求項１６】前記情報処理方法において、さらに、
コピーの可否を設定したコピー制御情報に基づいて、前記コンテンツデータを格納したコンテンツ格納記録媒体からのコンテンツデータのコピーの可否を判定するステップを有し、
前記コピー制御情報には、コピーの可否とともに、コピーの許容回数が設定されていることを示す態様としての、コピー数制限ありを示す情報を含み、
前記コピー制御情報がコピー数制限ありを示す情報であるか否かを判定し、
コピー数制限ありを示すコピー制御情報であると判定されたことを条件として、前記他の情報処理装置または他の記録媒体に対するコピー可否判定処理を、前記コンテンツデータ毎のコピー可能回数を設定したコピー履歴テーブルに基づいて実行することを特徴とする請求項１２に記載の情報処理方法。
【請求項１７】前記情報処理方法は、さらに、
コンテンツデータの受信に際して、コピーの可否を設定したコピー制御情報を受信し、
コピー制御情報が、コピーの許容回数が設定されていることを示す態様としてのコピー数制限ありを示す情報である場合に、前記コピー履歴テーブルを生成して、生成したコピー履歴テーブルに基づくコピー制御処理を実行することを特徴とする請求項１２に記載の情報処理方法。
【請求項１８】前記情報処理方法は、さらに、
コンテンツデータの受信に際して、コピーの可否を設定したコピー制御情報を受信し、コピー制御情報が、コピーの許容回数が設定されていることを示す態様としてのコピー数制限ありを示す情報であり、さらにコピーの許容回数の指定データが前記コピー制御情報中に含まれる場合に、前記コピー履歴テーブルを、前記コピー制御情報中のコピーの許容回数データに基づいて生成して、生成したコピー履歴テーブルに基づくコピー制御処理を実行することを特徴とする請求項１７に記載の情報処理方法。
【請求項１９】前記情報処理方法は、さらに、
コンテンツデータの受信に際して、コピーの可否を設定したコピー制御情報を受信し、コピー制御情報が、コピーの許容回数が設定されていることを示す態様としてのコピー数制限ありを示す情報であり、コピーの許容回数の指定データが前記コピー制御情報中に含まれない場合に、前記コピー履歴テーブルを、前記情報処理装置に予め設定済みのコピー許容回数データに基づいて生成して、生成したコピー履歴テーブルに基づくコピー制御処理を実行することを特徴とする請求項１７に記載の情報処理方法。
【請求項２０】前記情報処理方法は、さらに、
コンテンツデータの受信に際して、受信コンテンツに対応するコピー履歴テーブルを受信し、受信したコピー履歴テーブルに基づくコピー制御処理を実行することを特徴とする請求項１２に記載の情報処理方法。
【請求項２１】コンテンツデータを格納した情報記録媒体であり、
前記記録媒体に格納されたコンテンツデータについて、コンテンツデータ毎のコピー可能回数を設定したコピー履歴テーブルを格納したことを特徴とする情報記録媒体。
【請求項２２】前記コピー履歴テーブルには、コピー可能回数に対応して設定されるコピー番号と、コピー番号

毎に対応して設定されるコピー格納先メディアＩＤ設定欄を有することを特徴とする請求項２１に記載の情報記録媒体。

【請求項２３】前記コピー履歴テーブルは、
前記コンテンツ格納記録媒体の識別子と、前記情報処理装置に格納されたマスターキーとに基づいて生成される暗号化キーで暗号化されて格納された構成であることを特徴とする請求項２１に記載の情報記録媒体。

【請求項２４】前記コピー履歴テーブルには、複数のコンテンツデータの各々に対応して許容可能な個別のコピー可能回数が設定された構成であることを特徴とする請求項２１に記載の情報記録媒体。

【請求項２５】コンテンツ格納記録媒体に格納されたコンテンツデータについての、他の情報処理装置または他の記録媒体に対するコピー可否判定処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、
コンテンツデータのコピー先となる他の情報処理装置または他の記録媒体の識別子を前記コピー格納先メディアＩＤ欄に記録可能か否かを判定するステップと、
前記コピー格納先メディアＩＤ欄に記録可能であることを条件として前記コンテンツ格納記録媒体からのコピーが可能であると判定するステップと、
を有することを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報処理装置、情報処理方法、および情報記録媒体、並びにプログラム提供媒体に関し、特に、データ記録再生可能な記録媒体に対するデータ書き込み、データ再生処理における違法コピーを防止することを可能とした情報処理装置、情報処理方法、および情報記録媒体、並びにプログラム提供媒体に関する。

【０００２】

【従来の技術】ディジタル信号処理技術の進歩、発展に伴い、近年においては、情報を、ディジタル的に記録する記録装置や記録媒体が普及しつつある。このようなディジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにディジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通することになると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなディジタルデータの不正なコピーを防ぐため、ディジタル記録装置および記録媒体に違法なコピーを防止するための様々な仕組み（システム）が導入されている。

【０００３】例えば、ＭＤ（ミニディスク）（ＭＤは商標）装置において、違法なコピーを防止する方法として、ＳＣＭＳ(Serial Copy Management System)が採用されている。ＳＣＭＳは、データ再生側において、オーディオデータとともにＳＣＭＳ信号をディジタルインタフェース（ＤＩＦ）から出力し、データ記録側において、再生側からのＳＣＭＳ信号に基づいて、再生側からのオーディオデータの記録を制御することにより違法なコピーを防止するシステムである。

【０００４】具体的にはＳＣＭＳ信号は、オーディオデータが、何度でもコピーが許容されるコピーフリー（copy free）のデータであるか、１度だけコピーが許されている（copy once allowed）データであるか、またはコピーが禁止されている（copy prohibited）データであるかを表す信号である。データ記録側において、ディジタルインタフェース（ＤＩＦ）からオーディオデータを受信すると、そのオーディオデータとともに送信されるＳＣＭＳ信号を検出する。そして、ＳＣＭＳ信号が、コピーフリー（copy free）となっている場合には、オーディオデータをＳＣＭＳ信号とともにミニディスクに記録する。また、ＳＣＭＳ信号が、コピーを１度のみ許可（copy once allowed）となっている場合には、ＳＣＭＳ信号をコピー禁止（copy prohibited）に変更して、オーディオデータとともに、ミニディスクに記録する。さらに、ＳＣＭＳ信号が、コピー禁止（copy prohibited）となっている場合には、オーディオデータの記録を行わない。このようなＳＣＭＳを使用した制御を行なうことで、ミニディスク装置では、ＳＣＭＳによって、著作権を有するオーディオデータが、違法にコピーされるのを防止するようになっている。

【０００５】

【発明が解決しようとする課題】しかしながら、上記のＳＣＭＳで行えるのは、コピーの世代管理のみである。例えば、コピーを１度のみ許可（copy once allowed）とされるデータは、子から孫を作るコピーが禁じられるのみであり、元データからは複数のコピー（子）を作ることが可能である。今後のネットワーク社会においては、音楽などのコンテンツデータに対し、よりきめ細かくコピーの制御を行いたいという要望が著作権者などから出されている。本発明は、データごとに作られるコピー（子）の数を制限できる情報処理装置、情報処理方法、および情報記録媒体、並びにプログラム提供媒体を提供することを目的とする。

【０００６】

【課題を解決するための手段】本発明の第１の側面は、コンテンツデータを格納したコンテンツ格納記録媒体からコンテンツデータを他の情報処理装置または他の記録媒体に出力可能な情報処理装置において、前記コンテンツ格納記録媒体に格納されたコンテンツデータについての、前記他の情報処理装置または他の記録媒体に対するコピー可否判定処理を、前記コンテンツデータ毎のコピ

ー可能回数を設定したコピー履歴テーブルに基づいて判定する制御手段を有することを特徴とする情報処理装置にある。

【０００７】さらに、本発明の情報処理装置の一実施態様において、前記コピー履歴テーブルには、コピー可能回数に対応して設定されるコピー番号と、コピー番号毎に対応して設定されるコピー格納先メディアＩＤ設定欄を有し、前記制御手段は、コンテンツデータのコピー先となる他の情報処理装置または他の記録媒体の識別子を前記コピー格納先メディアＩＤ欄に記録したことを条件として前記コンテンツ格納記録媒体からのコピーを実行する構成を有することを特徴とする。

【０００８】さらに、本発明の情報処理装置の一実施態様において、前記コピー履歴テーブルは、前記コンテンツ格納記録媒体、または該コンテンツ格納記録媒体を装着した情報処理装置内のメモリに暗号化されたデータとして格納された構成であることを特徴とする。

【０００９】さらに、本発明の情報処理装置の一実施態様において、前記コピー履歴テーブルの暗号化キーは、前記コンテンツ格納記録媒体の識別子と、前記情報処理装置に格納されたマスターキーとに基づいて生成される暗号化キーであることを特徴とする。

【００１０】さらに、本発明の情報処理装置の一実施態様において、前記コピー履歴テーブルには、コピー可能回数に対応して設定されるコピー番号と、コピー番号毎に対応して設定されるコピー格納先メディアＩＤ設定欄を有し、前記制御手段は、コンテンツデータのコピー先となる他の情報処理装置または他の記録媒体の識別子と同一の識別子が既に前記コピー格納先メディアＩＤ欄に記録されている場合には、同一の識別子を有する他の情報処理装置または他の記録媒体に対する前記コンテンツ格納記録媒体からのコピーを実行する構成を有することを特徴とする。

【００１１】さらに、本発明の情報処理装置の一実施態様において、前記コピー履歴テーブルには、複数のコンテンツデータの各々に対応して許容可能な個別のコピー可能回数が設定された構成であることを特徴とする。

【００１２】さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、さらに、コピーの可否を設定したコピー制御情報に基づいて、前記コンテンツデータを格納したコンテンツ格納記録媒体からのコンテンツデータのコピーの可否を判定する構成を有し、前記コピー制御情報には、コピーの可否とともに、コピーの許容回数が設定されていることを示す態様としての、コピー数制限ありを示す情報を含み、前記制御手段は、前記コピー制御情報がコピー数制限ありを示す情報であるか否かを判定し、コピー数制限ありを示すコピー制御情報であると判定されたことを条件として、前記他の情報処理装置または他の記録媒体に対するコピー可否判定処理を、前記コンテンツデータ毎のコピー可能回数を設定したコピー履歴テーブルに基づいて実行する構成を有することを特徴とする。

【００１３】さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、さらに、コンテンツデータの受信に際して、コピーの可否を設定したコピー制御情報を受信し、コピー制御情報が、コピーの許容回数が設定されていることを示す態様としてのコピー数制限ありを示す情報である場合に、前記コピー履歴テーブルを生成して、生成したコピー履歴テーブルに基づくコピー制御処理を実行する構成を有することを特徴とする。

【００１４】さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、さらに、コンテンツデータの受信に際して、コピーの可否を設定したコピー制御情報を受信し、コピー制御情報が、コピーの許容回数が設定されていることを示す態様としてのコピー数制限ありを示す情報であり、さらにコピーの許容回数の指定データが前記コピー制御情報中に含まれる場合に、前記コピー履歴テーブルを、前記コピー制御情報中のコピーの許容回数データに基づいて生成して、生成したコピー履歴テーブルに基づくコピー制御処理を実行する構成を有することを特徴とする。

【００１５】さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、さらに、コンテンツデータの受信に際して、コピーの可否を設定したコピー制御情報を受信し、コピー制御情報が、コピーの許容回数が設定されていることを示す態様としてのコピー数制限ありを示す情報であり、コピーの許容回数の指定データが前記コピー制御情報中に含まれない場合に、前記コピー履歴テーブルを、前記情報処理装置に予め設定済みのコピー許容回数データに基づいて生成して、生成したコピー履歴テーブルに基づくコピー制御処理を実行する構成を有することを特徴とする。

【００１６】さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、さらに、コンテンツデータの受信に際して、受信コンテンツに対応するコピー履歴テーブルを受信し、受信したコピー履歴テーブルに基づくコピー制御処理を実行する構成を有することを特徴とする。

【００１７】さらに、本発明の第２の側面は、コンテンツデータを格納したコンテンツ格納記録媒体からコンテンツデータを他の情報処理装置または他の記録媒体に出力可能な情報処理装置における情報処理方法であり、前記コンテンツ格納記録媒体に格納されたコンテンツデータについての、前記他の情報処理装置または他の記録媒体に対するコピー可否判定処理を、前記コンテンツデータ毎のコピー可能回数を設定したコピー履歴テーブルに基づいて判定することを特徴とする情報処理方法にある。

【００１８】さらに、本発明の情報処理方法の一実施態

様において、前記コピー履歴テーブルには、コピー可能回数に対応して設定されるコピー番号と、コピー番号毎に対応して設定されるコピー格納先メディアＩＤ設定欄を有し、前記コピー可否判定処理は、コンテンツデータのコピー先となる他の情報処理装置または他の記録媒体の識別子を前記コピー格納先メディアＩＤ欄に記録可能か否かを判定するステップと、前記コピー格納先メディアＩＤ欄に記録可能であることを条件として前記コンテンツ格納記録媒体からのコピーを可能と判定するステップと、を含むことを特徴とする。

【００１９】さらに、本発明の情報処理方法の一実施態様において、前記コンテンツ格納記録媒体の識別子と、前記情報処理装置に格納されたマスターキーとに基づいて、暗号化キーを生成し、前記暗号化キーに基づいて前記コピー履歴テーブルを暗号化して前記コンテンツ格納記録媒体、または該コンテンツ格納記録媒体を装着した情報処理装置内のメモリに格納する処理を実行することを特徴とする。

【００２０】さらに、本発明の情報処理方法の一実施態様において、前記コピー履歴テーブルには、コピー可能回数に対応して設定されるコピー番号と、コピー番号毎に対応して設定されるコピー格納先メディアＩＤ設定欄を有し、前記コピー可否判定処理は、コンテンツデータのコピー先となる他の情報処理装置または他の記録媒体の識別子と同一の識別子が既に前記コピー格納先メディアＩＤ欄に記録されている場合には、同一の識別子を有する他の情報処理装置または他の記録媒体に対する前記コンテンツ格納記録媒体からのコピーを実行可と判定することを特徴とする。

【００２１】さらに、本発明の情報処理方法の一実施態様において、コピーの可否を設定したコピー制御情報に基づいて、前記コンテンツデータを格納したコンテンツ格納記録媒体からのコンテンツデータのコピーの可否を判定するステップを有し、前記コピー制御情報には、コピーの可否とともに、コピーの許容回数が設定されていることを示す態様としての、コピー数制限ありを示す情報を含み、前記コピー制御情報がコピー数制限ありを示す情報であるか否かを判定し、コピー数制限ありを示すコピー制御情報であると判定されたことを条件として、前記他の情報処理装置または他の記録媒体に対するコピー可否判定処理を、前記コンテンツデータ毎のコピー可能回数を設定したコピー履歴テーブルに基づいて実行することを特徴とする。

【００２２】さらに、本発明の情報処理方法の一実施態様において、コンテンツデータの受信に際して、コピーの可否を設定したコピー制御情報を受信し、コピー制御情報が、コピーの許容回数が設定されていることを示す態様としてのコピー数制限ありを示す情報である場合に、前記コピー履歴テーブルを生成して、生成したコピー履歴テーブルに基づくコピー制御処理を実行することを特徴とする。

【００２３】さらに、本発明の情報処理方法の一実施態様において、コンテンツデータの受信に際して、コピーの可否を設定したコピー制御情報を受信し、コピー制御情報が、コピーの許容回数が設定されていることを示す態様としてのコピー数制限ありを示す情報であり、さらにコピーの許容回数の指定データが前記コピー制御情報中に含まれる場合に、前記コピー履歴テーブルを、前記コピー制御情報中のコピーの許容回数データに基づいて生成して、生成したコピー履歴テーブルに基づくコピー制御処理を実行することを特徴とする。

【００２４】さらに、本発明の情報処理方法の一実施態様において、コンテンツデータの受信に際して、コピーの可否を設定したコピー制御情報を受信し、コピー制御情報が、コピーの許容回数が設定されていることを示す態様としてのコピー数制限ありを示す情報であり、コピーの許容回数の指定データが前記コピー制御情報中に含まれない場合に、前記コピー履歴テーブルを、前記情報処理装置に予め設定済みのコピー許容回数データに基づいて生成して、生成したコピー履歴テーブルに基づくコピー制御処理を実行することを特徴とする。

【００２５】さらに、本発明の情報処理方法の一実施態様において、コンテンツデータの受信に際して、受信コンテンツに対応するコピー履歴テーブルを受信し、受信したコピー履歴テーブルに基づくコピー制御処理を実行することを特徴とする。

【００２６】さらに、本発明の第３の側面は、コンテンツデータを格納した情報記録媒体であり、前記記録媒体に格納されたコンテンツデータについて、コンテンツデータ毎のコピー可能回数を設定したコピー履歴テーブルを格納したことを特徴とする情報記録媒体にある。

【００２７】さらに、本発明の情報記録媒体の一実施態様において、前記コピー履歴テーブルには、コピー可能回数に対応して設定されるコピー番号と、コピー番号毎に対応して設定されるコピー格納先メディアＩＤ設定欄を有することを特徴とする。

【００２８】さらに、本発明の情報記録媒体の一実施態様において、前記コピー履歴テーブルは、前記コンテンツ格納記録媒体の識別子と、前記情報処理装置に格納されたマスターキーとに基づいて生成される暗号化キーで暗号化されて格納された構成であることを特徴とする。

【００２９】さらに、本発明の情報記録媒体の一実施態様において、前記コピー履歴テーブルには、複数のコンテンツデータの各々に対応して許容可能な個別のコピー可能回数が設定された構成であることを特徴とする。

【００３０】さらに、本発明の第４の側面は、コンテンツ格納記録媒体に格納されたコンテンツデータについての、他の情報処理装置または他の記録媒体に対するコピー可否判定処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提

供媒体であって、前記コンピュータ・プログラムは、コンテンツデータのコピー先となる他の情報処理装置または他の記録媒体の識別子を前記コピー格納先メディアＩＤ欄に記録可能か否かを判定するステップと、前記コピー格納先メディアＩＤ欄に記録可能であることを条件として前記コンテンツ格納記録媒体からのコピーが可能であると判定するステップと、を有することを特徴とするプログラム提供媒体にある。

【００３１】なお、本発明の第４の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、ＣＤやＦＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【００３２】このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【００３３】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００３４】

【発明の実施の形態】［実施例１］図１は、本発明を適用した情報処理装置としての記録再生装置１００の一実施例形態の構成を示すブロック図である。記録再生装置１００は、入出力Ｉ／Ｆ(Interface)１２０、ＭＰＥＧ(Moving Picture Experts Group)コーデック１３０、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を備えた入出力Ｉ／Ｆ(Interface)１４０、暗号処理手段１５０、ＣＰＵ(Central Processing Unit)１７０、メモリ１８０、記録媒体１９５に対する記録媒体インタフェース（Ｉ／Ｆ）１９０を有し、これらはバス１１０によって相互に接続されている。

【００３５】入出力Ｉ／Ｆ１２０は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するディジタル信号を受信し、バス１１０上に出力するとともに、バス１１０上のディジタル信号を受信し、外部に出力する。ＭＰＥＧコーデック１３０は、バス１１０を介して供給されるＭＰＥＧ符号化されたデータを、ＭＰＥＧデコードし、入出力Ｉ／Ｆ１４０に出力するとともに、入出力Ｉ／Ｆ１４０から供給されるディジタル信号をＭＰＥＧエンコードしてバス１１０上に出力する。入出力Ｉ／Ｆ１４０は、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を内蔵している。入出力Ｉ／Ｆ１４０は、外部から供給されるコンテンツとしてのアナログ信号を受信し、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＡ／Ｄ(Analog Digital)変換することで、ディジタル信号として、ＭＰＥＧコーデック１３０に出力するとともに、ＭＰＥＧコーデック１３０からのディジタル信号を、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＤ／Ａ(Digital Analog)変換することで、アナログ信号として、外部に出力する。

【００３６】暗号処理手段１５０は、例えば、１チップのＬＳＩ(Large Scale IntegratedCurcuit)で構成され、バス１１０を介して供給されるコンテンツとしてのディジタル信号を暗号化し、または復号し、バス１１０上に出力する構成を持つ。なお、暗号処理手段１５０は１チップＬＳＩに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構成による処理手段としての構成については後段で説明する。

【００３７】ＣＰＵ１７０は、メモリ１８０に記憶されたプログラムを実行することで、ＭＰＥＧコーデック１３０や暗号処理手段１５０等を制御する。さらに、後段で詳細に説明するが本発明に特有のコピー履歴テーブルの読み出し処理、さらにコピー履歴テーブルを参照したコピー実行の可否判定処理等の制御手段の主要構成要素として機能する。メモリ１８０は、例えば、不揮発性メモリで、ＣＰＵ１７０が実行するプログラムや、ＣＰＵ１７０の動作上必要なデータを記憶する。例えば、後段で詳細に説明するコピー実行の可否判定処理プログラムを格納する。記録媒体インタフェース１９０は、デジタルデータを記録再生可能な記録媒体１９５を駆動することにより、記録媒体１９５からディジタルデータを読み出し（再生し）、バス１１０上に出力するとともに、バス１１０を介して供給されるディジタルデータを、記録媒体１９５に供給して記録させる。

【００３８】記録媒体１９５は、例えば、ＤＶＤ、ＣＤ等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはＲＡＭ等の半導体メモリ等のディジタルデータの記憶可能な媒体であり、本実施の形態では、記録媒体インタフェース１９０対して着脱可能な構成であるとする。但し、記録媒体１９５は、記録再生装置１００に内蔵する構成としてもよい。

【００３９】なお、記録媒体１９５には個々の記録媒体を識別するための媒体識別情報（メディアＩＤ）が記録されている。具体的には、本出願人による先の特許出願、特開平１１－２２４４６１号公報（特願平１０－２５３１０号）において説明しているが、個々の記録媒体を識別する為の媒体識別情報を、他のデータとともに記録媒体に記録し、この媒体識別情報のライセンスを受けた装置であることを条件として、その条件が満たされた場合にのみ記録媒体の媒体識別情報へのアクセスが可能となる。

【００４０】この方法では、記録媒体上のデータは、媒

体識別情報とライセンスを受けることにより得られる秘密キー（マスターキー）により暗号化され、ライセンスを受けていない装置が、この暗号化されたデータを読み出したとしても、意味のあるデータを得ることができないようになっている。例えば前述のデバイスキーを用いて復号キーを生成する構成として、ライセンスを受けたデバイスに復号キーを生成可能なデバイスキーを付与する構成とする。なお、装置はライセンスを受ける際、不正な複製（違法コピー）ができないように、その動作が規定される。

【００４１】ライセンスを受けていない装置は、媒体識別情報にアクセスできず、また、媒体識別情報は個々の媒体毎に個別の値となっているため、ライセンスを受けていない装置が、記録媒体に記録されている、暗号化されたデータのすべてを新たな記録媒体に複製したとしても、そのようにして作成された記録媒体に記録されたデータは、ライセンスを受けていない装置は勿論、ライセンスを受けた装置においても、正しく復号することができないから、実質的に、違法コピーが防止されることになる。

【００４２】なお、本発明の記録再生装置の構成例としては図１に示す構成の他に図２に示す構成が可能である。図２に示す記録再生装置２００では、記録媒体１９５はドライブ装置としての記録媒体インタフェース（Ｉ／Ｆ）１９０とともに記録再生装置２００に内蔵されており、外部から入力されるデータ書き込みは、内蔵された記録媒体１９５に対して実行される。

【００４３】図３に、本発明を利用した機器を用いたデータのコピーを行う場合の機器構成の一例を示す。図３においては、図１に示した記録再生機器を２台用いて、これら２台の機器をデジタルバス３００を用いて接続し、記録媒体(メディア１)に記録されているコンテンツデータを記録媒体(メディア２)にコピーする様子を示している。

【００４４】記録媒体(メディア１)にはあらかじめ、１つあるいは複数のコンテンツデータが記録され、それぞれのコンテンツデータについて、そのデータを元（親）として作成してよいコピー（子）の個数が決められている。この個数は、システムで一意に設定してもよいし、コンテンツデータごとに個別に設定してもよい。

【００４５】さらに、記録媒体(メディア１)には、図４に示すコピー履歴テーブルが格納される。このテーブルは、たとえばその記録媒体に格納されているデータが、始めてコピーされる際に記録再生機器により生成される構成としてもよいし、記録媒体(メディア１)にコンテンツデータが記録される際に記録再生機器により作られるようにしてもよい。

【００４６】コピー履歴テーブルには、コンテンツデータの識別情報であるコンテンツＩＤ、そのデータから作られたコピー（子）の番号、コピーの格納先の記録媒体の識別情報であるメディアＩＤが格納される。

【００４７】たとえば図４に示したコピー履歴のテーブルの例では、この記録媒体にはコンテンツＩＤ：12345678とabcd1234というコンテンツデータが記録されており、コンテンツＩＤ＝12345678のデータは、コピー番号の欄が１～Ｎまで設定されており、Ｎ個までコピーを作ることが許されている。図４の例では、コンテンツＩＤ＝12345678のデータは、コピー格納先メディアＩＤの欄に記録されているように、既に記録媒体識別番号（メディアＩＤ）がabcdefghと87654321という識別情報を持つ記録媒体にコピーが行われている。このテーブルを持つ記録媒体に格納されたコンテンツのコピーが実行されると、テーブルの対応コンテンツＩＤのコピー格納先メディアＩＤ欄にコピー番号１からＮまで、順次、コピーデータの格納先となるメディアＩＤが記録される。図４の例では、コピー番号：３以降のコピーはまだ作られていないため、コピー番号３からＮについては空欄となっている。同様にコンテンツＩＤ＝abcd1234のコンテンツは、Ｍ個までコピーを作ることが許されており、識別番号87654321の記録媒体に１つコピーが行われたことを意味している。

【００４８】なお、後段で説明するが、記録媒体が記録再生装置に内蔵された構成である場合は、図４のコピー履歴テーブルのコピー格納先メディアＩＤ欄にコピー格納先記録再生装置（情報処理装置）の識別子を格納する構成としてもよい。また、コピー履歴テーブルを記録媒体自体に格納せず、記録再生装置内のメモリに格納する構成として、必要に応じて読み出す構成としてもよい。

【００４９】本発明の情報処理装置は、記録媒体に格納されたコンテンツデータについて、他の情報処理装置または他の記録媒体に対するコピー可否判定処理を、上述したコンテンツデータ毎のコピー可能回数を設定したコピー履歴テーブルに基づいて判定する。この判定処理は、図１または図２の記録再生装置構成における制御手段によって実行される。具体的には、制御手段の構成要素はＣＰＵ１７０であり、メモリ１８０に格納された処理プログラムに従ってＣＰＵ１７０が処理を実行する。

【００５０】図４に示すように、コピー履歴テーブルには、コピー可能回数に対応して設定されるコピー番号と、コピー番号毎に対応して設定されるコピー格納先メディアＩＤ設定欄を有し、制御手段としてのＣＰＵ１７０は、コンテンツデータのコピー先となる他の情報処理装置または他の記録媒体の識別子を前記コピー格納先メディアＩＤ欄に記録する処理を実行し、ＩＤが新たに記録されたことを条件としてコンテンツ格納記録媒体からのコピーを実行する。

【００５１】ただし、コンテンツデータのコピー先となる他の情報処理装置または他の記録媒体の識別子と同一の識別子が既に前記コピー格納先メディアＩＤ欄に記録されている場合には、同一の識別子を有する他の情報処

理装置または他の記録媒体に対するコンテンツ格納記録媒体からのコピーは繰り返し実行可能であり、新たな識別子を持つ他の情報処理装置または他の記録媒体に対するコピー時にのみ、そのＩＤをコピー履歴テーブルに記録する処理を実行する。

【００５２】なお、本実施例では、記録媒体（メディア１）は、例えば図５に示すような中心孔５０１、ＲＡＭ領域５０２を有するＲＡＭメディアとすることが可能であり、この場合、コンテンツデータおよびコピー履歴テーブルはともにＲＡＭメディア上に格納する。また、記録媒体（メディア１）は、図６に示すような中心孔６０１、ＲＡＭ領域６０２、ＲＯＭ領域６０３を有するＲＡＭとＲＯＭの混在メディアとした構成も可能であり、この場合、コンテンツデータをＲＯＭ領域６０３に格納し、コピー履歴テーブルをＲＡＭ領域６０２に格納するように構成してもよい。

【００５３】また、記録媒体（メディア１）は、図７に示すような、カートリッジ７０１にＲＯＭまたはＲＡＭからなる光ディスク７０２を収納し、さらに不揮発メモリを有するＩＣチップ７０３を持つ構成、すなわち、ＲＯＭメディアと書き換え可能な記憶領域を持つＩＣチップが組み合わさった記録媒体とすることも可能であり、この場合、例えばコンテンツデータは光ディスク７０２のＲＯＭ領域に、コピー履歴テーブルをＩＣチップ７０３にそれぞれ格納する。さらに、記録媒体（メディア１）は、図８に示すような記録可能な領域を持つ１つもしくは複数のＩＣチップ８０４を有するカートリッジ８０１とすることも可能である。カートリッジ８０１には、記録再生機器接続用の入出力端子８０２、メモリコントロール用ＩＣチップ８０３を有する。このカートリッジ８０１においては、コンテンツデータ、コピー履歴テーブルともにＩＣチップ８０４に格納される。

【００５４】図９に、図３の構成を用いて記録再生機器Ａ(デバイスＡ)に接続された記録媒体(メディア１)上のコンテンツデータを記録再生機器Ｂ(デバイスＢ)に接続された記録媒体(メディア２)にコピーする場合の処理フローを示す。一連の処理は、たとえば、記録再生機器Ｂ(デバイスＢ)から記録再生機器ＡデバイスＡ)に対してあるコンテンツデータのコピーを要求するコマンドを送信することによって開始される。

【００５５】図９のステップＳ９０１において、記録再生機器Ａ（デバイスＡ)と記録再生機器Ｂ(デバイスＢ)はお互いの正当性を確認するために、相互認証および鍵共有プロトコルを実行し、このプロトコルを用いて共有した暗号鍵をそれ以降の通信に用いる。ただし、システムが高度のセキュリティを必要としない場合には、このプロトコルを行わなくてもよい。

【００５６】相互認証のプロトコルの例としては、ISO/IEC 9798-2に代表される、共通鍵暗号を用いるもの、ISO/IEC 9798-3 に代表される、公開鍵暗号を用いるもの、ISO/IEC 9798-4に代表される、暗号学的チェック関数を用いるものなどが挙げられる。

【００５７】図１０は、暗号学的チェック関数を用いた相互認証および暗号鍵共有のための方法のひとつを本実施例に用いたものである。図１０において、記録再生機器Ａ(デバイスＡ)と記録再生機器Ｂ(デバイスＢ)は、システム共通の秘密鍵：ＤＫを、たとえばメモリ１８０に格納している。まず、デバイスＢは乱数Ｒ_Ｂを発生し、デバイスＡに送る。

【００５８】次にデバイスＡは、乱数Ｒ_Ａ、Ｓ_Ａを生成し、Ｒ_Ａ,Ｓ_ＡとともにＭＡＣ(ＤＫ,Ｒ_Ａ || Ｒ_Ｂ || Ｓ_Ａ)をデバイスＢに送る。ＭＡＣ(ＤＫ,Ｒ_Ａ || Ｒ_Ｂ || Ｓ_Ａ)は、暗号学的チェック関数に鍵としてシステム共通の秘密鍵：ＤＫを、データとしてＲ_Ａ || Ｒ_Ｂ || Ｓ_Ａを入力することを表す。暗号学的チェック関数は、ISO/IEC 9797 に示されているように、FIPS 46-2 のデータ暗号化規格（Data Encryption Standard, DES）を用いて構成することが可能である。なお、図１０における記号 || は連結を表している。

【００５９】デバイスＢは、受信したデータを用いて自分でもＭＡＣ(ＤＫ,Ｒ_Ａ || Ｒ_Ｂ|| Ｓ_Ａ)を計算し、これが受信したものと一致するかを検査する。一致すれば、デバイスＡが正当なものであるとして認め、処理を続けるが、一致しなければデバイスＢが不正なものであると判断して処理を中止する。

【００６０】次にデバイスＢは乱数Ｓ_Ｂを生成し、これとＭＡＣ(ＤＫ,Ｒ_Ｂ || Ｒ_Ａ ||Ｓ_Ｂ)をデバイスＡに送る。

【００６１】デバイスＡも受信したデータを用いて自分でＭＡＣ(ＤＫ,Ｒ_Ｂ || Ｒ_Ａ ||Ｓ_Ｂ)を計算し、受信したものと一致するかを確認する。一致すれば、デバイスＢが正当なものであるとして認め、処理を続けるが、一致しなければデバイスＢが不正なものと判断して処理を中止する。

【００６２】最後に、双方がＭＡＣ(ＤＫ，Ｓ_Ａ || Ｓ_Ｂ)を計算し、これをそのセッションにおけるセッションキーとして使用する。

【００６３】上記のようにすることにより、２つの記録再生装置は互いの正当性を検査することができ、またセッションキーを安全に共有することができたので、例えば、このセッションキーを鍵として、そのセッションの通信内容を暗号化することにより安全に相手に送信することが可能となる。

【００６４】図１１は、公開鍵暗号、具体的には楕円曲線暗号を用いた認証技術を本実施例に適用したものである。

【００６５】図１１において、デバイスＡおよびデバイスＢは、それぞれ自分の識別情報であるＩＤと、自分の公開鍵証明書、およびリボケーションリストまたはレジストレーションリストを持っている。公開鍵証明書は、

図１２に示すように、そのエンティティのＩＤと、公開鍵に対し、信頼できるセンタがデジタル署名を施したデータである。

【００６６】リボケーションリストは、不正者リストあるいはブラックリストとも呼ばれ、図１３に示すように、その装置の秘密鍵が露呈してしまったもののＩＤがリストアップされ、単調に増加するバージョンナンバーとともにセンタのデジタル署名が施されたものである。

【００６７】これに対し、レジストレーションリストは、正当者リストあるいは登録リストとも呼ばれ、図１４に示すように、その時点で信頼できる（秘密が露呈していない）装置のＩＤがリストアップされ、単調に増加するバージョンナンバーとともにセンタのデジタル署名が施されたものである。

【００６８】図１１において、デバイスＢは乱数Ｒ_Ｂを発生させ、デバイスＡに送る。デバイスＡは、乱数Ｋ_ＡおよびＲ_Ａを発生させ、楕円曲線Ｅ上でシステム共通の点（ベースポイント）であるＧとＫ_Ａを乗算してＶ_Ａを計算し、さらに自分の秘密鍵（PriKey_Ａ）を用いてデータＲ_Ａ || Ｒ_Ｂ || Ｖ_Ａに対して施した署名とともに、公開鍵証明書（Cert_Ａ）とＲ_Ａ || Ｒ_Ｂ || Ｖ_Ａをデバイスに送る。

【００６９】デバイスＢは、デバイスＡの公開鍵証明書の正当性、デバイスＡが作成した署名の正当性を検査する。そして、自分がリボケーションリストを格納していれば、相手のＩＤがリボケーションリストに載っていないことを、また、自分がレジストレーションリストを格納していれば、相手のＩＤがレジストレーションリストに登録されていることを確認する。以上の確認が正常にできなければ、デバイスＢはデバイスＡが不正者であると判断して処理を終了する。以上の確認が正常にできれば、デバイスＢは、乱数Ｋ_Ｂを生成して、デバイスＡが行ったのと同様な計算を行い、公開鍵証明書（Cert_Ｂ）とＲ_Ｂ,Ｒ_Ａ,Ｖ_ＢとともにデータＲ_Ｂ || Ｒ_Ａ || Ｖ_Ｂに対して施した署名をデバイスＡに送る。

【００７０】デバイスＡでは、上記のデバイスＢが行ったのと同様の検査を受信したデータに対して行い、すべての検査が正常に終了したときのみ処理を継続する。

【００７１】この後、デバイスＡではＫ_ＡとＶ_Ｂを、デバイスＢではＫ_ＢとＶ_Ａを、それぞれ楕円曲線Ｅ上で乗算してセッションキーＫ_Ｓを得る。セッションキーの使用方法については、上述の暗号学的チェック関数を用いた相互認証の場合と同様である。

【００７２】なお、楕円曲線上の乗算やデジタル署名の生成および検査方法については、現在IEEE P1363 で規格制定中であり、そのドラフトに詳細が記されている。

【００７３】図９に戻り、図３の構成において、記録再生機器Ａ(デバイスＡ)に接続された記録媒体(メディア１)上のコンテンツデータを記録再生機器Ｂ(デバイスＢ)に接続された記録媒体(メディア２)にコピーする場合の処理フローの説明を続ける。ステップＳ９０２において、デバイスＢはデバイスＡに、記録媒体(メディア２)の識別情報（メディアＩＤ）を送信する。

【００７４】ステップＳ９０３において、デバイスＡは、記録媒体(メディア１)からコピー履歴テーブルを読出し、そのコンテンツデータをデバイスＢに接続された記録媒体(メディア２)にコピーしてよいか否かを判断する。

【００７５】この判断は、基本的には、コピー履歴テーブルの、そのコンテンツに対応するコピー先メディアＩＤの欄に空欄があるかどうか、すなわち、既に許容個数までコピーが作成されていないかどうかを用いて判断される。空欄があれば、コピーが許され、空欄がなければコピーは許可されない。

【００７６】また、すでにそのコンテンツデータのコピーが行われ、コピー履歴テーブルにそのＩＤが記録されている記録媒体に対して行われるコピーについては、コピー（子）の個数を増やさないと決めることも可能である。即ち、たとえば図４のコピー履歴テーブルにおいてコンテンツＩＤ 12345678 のデータのコピー格納先メディアＩＤの欄がＮ個すべて埋まっていた場合、基本的にはこのデータからの新たなコピーは許可されないが、コピー格納先メディアＩＤに記されたメディアＩＤを持つ記録媒体に対するコピーのみは許可されるとするものである。ステップＳ９０３の詳細を図１５の処理フローを用いて説明する。

【００７７】図１５は、本出願と同一の出願人に係る先の特許出願である特開平１１－２２４４６１号公報で提案した方式、すなわち複数の記録再生機器に共通に格納された秘密鍵（マスターキー）と記録媒体固有情報から暗号化キーおよび復号キーを生成する手法に、本発明のコピー制御情報によるコピー制御処理を適用した場合の処理、すなわち記録媒体に格納したコピー履歴テーブル（図４参照）の暗号化、復号処理に秘密鍵（マスターキー）と記録媒体固有情報（メディアＩＤ）とから生成した鍵を用いる処理フローである。

【００７８】ステップＳ１５０１において、コピー履歴テーブルを格納した記録媒体をアクセスしたデバイス（図３の例では、記録再生機器Ａ（デバイスＡ））はメディア１のメディアＩＤを読み出す。

【００７９】次に、デバイスＡは、ステップＳ１５０２において、メディア１のメディアＩＤと自身が格納しているマスターキーに基づいて暗号鍵を生成する。さらに、ステップＳ１５０３で、デバイスはメディア１から暗号化されて格納されているコピー履歴テーブルを読み出す。ステップＳ１５０４において、デバイスＡはステップＳ１５０２で生成した暗号鍵を用いてコピー履歴テーブルを復号する。さらに、ステップＳ１５０５において、デバイスＡは上述した手順に従ってコピーの許可、不許可を判定する。すなわち、先に図４を用いて説明し

たコピー履歴テーブルにおいて、コピー対象のコンテンツＩＤのデータに対応して設定されたコピー番号の欄１～Ｘに対応するコピー格納先メディアＩＤの欄に空欄がある場合にのみ、コピー可と判断する。

【００８０】図９に戻り、処理フローの説明を続ける。ステップＳ９０３において、コピーが許可されない場合には、ステップＳ９０４乃至Ｓ９０６をスキップし、コピーを行わずに処理を終了する。一方、コピーが許可される場合にはステップＳ９０４に進む。

【００８１】ステップＳ９０４において、デバイスＡはコピー履歴テーブルを変更する必要があるかどうかを判定する。基本的には、コピーを行う場合にはコピー先のメディアＩＤを新たにテーブルに書き加える必要があるため、テーブルの変更が必要である。ただし、上述のように、同じメディアＩＤを持つ記録媒体へのコピーは何回行っても１回と考えるというルールの下では、今回のコピー先のメディアＩＤが既にテーブルのそのコンテンツデータに対応するコピー先メディアＩＤの欄に記録されている場合には、コピー履歴テーブルの変更は必要ではない。

【００８２】テーブルの変更が必要でない場合にはステップＳ９０５をスキップしてステップＳ９０６に進み、テーブルの変更が必要であればステップＳ９０５に進む。

【００８３】ステップＳ９０５では、デバイスＡはコピー履歴テーブルの変更を行う。具体的には、そのコンテンツデータに対応するコピー先メディアＩＤの空いている欄に今回コピーを作る記録媒体のメディアＩＤを追記する。ステップＳ９０５の詳細を図１６の処理フローを用いて説明する。

【００８４】図１６は、特開平１１－２２４４６１号公報で提案した方式、すなわち複数の記録再生機器に共通に格納された秘密鍵（マスターキー）と記録媒体固有情報から暗号化キーおよび復号キーを生成する手法を本発明のコピー履歴テーブルの変更（編集）処理に応用した場合の処理フローである。

【００８５】デバイスＡがメディア１上のコピー履歴テーブルを変更（編集）する処理において、図１６のステップＳ１６０１乃至Ｓ１６０４は、図１５のステップＳ１５０１乃至Ｓ１５０４と同一であり、記録再生機器に共通に格納された秘密鍵（マスターキー）と記録媒体固有情報としてのメデイアＩＤから復号キーを生成してコピー履歴テーブルを復号するステップである。

【００８６】ステップＳ１６０５において、実際にコピー履歴テーブルを編集する。ここでの編集は、先に図４を用いて説明したように、コピー対象となるコンテンツＩＤに対応して設定されたコピー格納先メディアＩＤ欄に、新たにコピーを実行するメディアのメディアＩＤを書き込む処理である。コピー履歴テーブルの編集が終了すると、ステップＳ１６０６において、先に生成したデータ暗号鍵を用いて編集後のコピー履歴テーブルを暗号化し、ステップＳ１６０７において暗号化したコピー履歴テーブルをメディア１に記録する。

【００８７】図９に戻り、処理フローの説明を続ける。上述のような処理に従ったコピー履歴テーブルの編集処理が終了すると、ステップＳ９０６に進む。ステップＳ９０６では、デバイスＡおよびデバイスＢの両機器はコンテンツデータのコピーを実行する。

【００８８】次に、図１７に、デバイスＡのメデイア１からデバイスＢのメディア２に対するコンテンツデータのコピー処理において、デバイスＡおよびデバイスＢの各々において実行される処理を簡潔に説明したフローを示す。以下、図１７の各処理ステップについて説明する。

【００８９】図１７も前述の図１５，１６と同様、本出願と同一の出願人に係る先の特許出願である特開平１１－２２４４６１号公報で提案した方式、すなわち複数の記録再生機器に共通に格納された秘密鍵（マスターキー）と記録媒体固有情報から暗号化キーおよび復号キーを生成する手法と、本発明のコピー制御情報によるコピー制御処理とを併せて実行した場合の処理フローである。また、図１７に示す処理フローは、デバイスＡがメディア１上のコピー履歴テーブルを用いてコピーの許可／不許可を判断し、コピー可である場合、すなわち、先に図４を用いて説明したコピー履歴テーブルにおいて、コピー対象のコンテンツＩＤのデータに対応して設定されたコピー番号の欄１～Ｘに対応して設定されたコピー格納先メディアＩＤの欄に空欄があり、コピー可と判断された場合に実行されるフローである。

【００９０】図１７の処理フローの左側はデバイスＡの処理、右側はデバイスＢの処理である。ステップＳ１７０１およびステップＳ１７２１において、デバイスＡおよびデバイスＢは、例えば先に図１０，１１を用いて説明した処理に従って、相互認証処理およびセッションキー生成処理を実行する。相互認証が成立し、セッションキーの生成に成功すると次のステップに進む。認証がエラーとなった場合は以下の処理は実行されない。

【００９１】ステップＳ１７０２において、デバイスＡはメディア１のメディアＩＤを読み出し、ステップＳ１７２２において、デバイスＢはメディア２のメディアＩＤを読み出す。デバイスＢはステップＳ１７２３において、読み出したメディア２のメディアＩＤをデバイスＡに送信する。この際、送信メディアＩＤはセッションキーで暗号化して送信してもよい。

【００９２】デバイスＡは、ステップＳ１７０３において、メディア１のメディアＩＤと自身が格納しているマスターキーに基づいて、メディア１上のデータを暗号化する暗号鍵（これを暗号鍵(1)と呼ぶ）を生成する。さらに、ステップＳ１７０４で、デバイスＡはメディア１からコピー履歴テーブルおよびコピー対象となるコンテ

ンツデータを読み出す。

【００９３】ステップＳ１７０５において、デバイスＡはメディア１からコピーすべきコンテンツデータと、コピー履歴テーブルとを先に生成した暗号鍵（暗号鍵(1)）を用いて復号する。

【００９４】ステップＳ１７０６において、デバイスＡは、ステップＳ１７２３でデバイスＢから、受信したメディア２のメディアＩＤに基づいてコピー履歴テーブルの更新処理を実行する。具体的には、先に図４を用いて説明したように、コピー対象となるコンテンツＩＤに対応して設定されたコピー格納先メディアＩＤ欄に、新たにコピーを実行するメディアのメディアＩＤを書き込む。

【００９５】ステップＳ１７０７において、デバイスＡはステップＳ１７０１でデバイスＢと共有したセッションキーを用いてコンテンツデータを暗号化し、ステップＳ１７０８で暗号化コンテンツデータをデバイスＢに送信する。なお、コンテンツデータを暗号化して伝送する方法として、××××××××××××××××××５社によって定められている、５ＣＤＴＣＰ(Five Company Digital Transmission Content Protection)（以下、適宜、ＤＴＣＰという）を用いてもよい。ここで、ＤＴＣＰについては、例えば、http://www.dtcp.comのURL(Uniform Resource Locator)で特定されるWebページにおいて、インフォメイショナルバージョン(Informational Version)の仕様書の取得が可能である。

【００９６】さらに、ステップＳ１７０９において、デバイスＡは、先に生成したデータ暗号鍵（暗号鍵(1)）を用いて編集後のコピー履歴テーブルを暗号化し、ステップＳ１７１０において暗号化したコピー履歴テーブルをメディア１に記録する。

【００９７】ステップＳ１７２４において、デバイスＢは暗号化されたコンテンツデータを受信する。ステップＳ１７２５において、デバイスＢはステップ１７２１で共有したセッションキーを用いて受信した暗号化コンテンツデータを復号する。

【００９８】次に、ステップＳ１７２６において、デバイスＢはメディア２から読み出したメディアＩＤと、自身が格納するマスターキーを用いてデータを暗号化する暗号鍵（暗号鍵(2)と呼ぶ）を生成する。ステップＳ１７２７において、デバイスＢは暗号鍵(2)を用いてコンテンツデータを暗号化し、ステップＳ１７２８において暗号化データをメディア２に記録する。

【００９９】以上の処理により、メディア１のコンテンツデータについて、許容された個数の範囲内の個数のコピーとなるようなコピーをメディア２に作成することができる。ステップＳ１７０６において、コピー履歴テーブルの更新処理、すなわち、コピー対象となるコンテンツＩＤに対応して設定されたコピー格納先メディアＩＤ欄に、新たにコピーを実行するメディアのメディアＩＤを書き込む処理が実行できない場合、すなわち、予めコピー履歴テーブルのコピー番号として設定された数を超える場合は、メディアＩＤを書き込めないことになり、以下の処理ステップＳ１７０７以下の処理が実行されない。この場合は、デバイスＢに対するコピー処理が実行されない。

【０１００】なお、上記の例では、コピー先の記録媒体（メディア２）が図１に示すようなリムーバブルメディアであることを前提としているが、これが図２の記録媒体のような、記録再生装置と一体型となっている記録媒体の場合、即ち、図１８に示す構成となっている場合には、メディア２のメディアＩＤの代わりに、コピー先の記録再生装置（デバイスＢ）の識別情報（デバイスＩＤ）を使用することも可能である。この場合、コピー履歴テーブルの、コピー先メディアＩＤの欄にはデバイスＩＤを記録してもよい。

【０１０１】さらに、コピー先の記録媒体が記録再生装置と一体型となっている場合のみならず、リムーバブル型の記録媒体の場合であっても、記録媒体のメディアＩＤの代わりに記録再生装置のデバイスＩＤを使用することは可能である。記録媒体上のデータが、それを記録した記録再生装置でのみ再生できるような暗号化をされる仕組みになっている場合に最も効果が大きいが、そうでない場合でも実施可能である。

【０１０２】また、上記の例では、コピー履歴テーブルを、記録媒体（メディア１）上に格納するようにしているが、これをコピー元の記録再生装置（デバイスＡ）内のたとえばメモリ１８０に格納するようにしてもよい。これも記録媒体上のデータが、それを記録した記録再生装置でのみ再生できるような暗号化をされる仕組みになっている場合に最も効果が大きいが、そうでない場合でも実施可能である。また、このようにすることにより、コピー元の記録媒体（メディア１）が書き込み可能な領域を持たない場合にも対応可能となる。

【０１０３】［実施例２］図１９は、本発明を適用した記録再生装置の別の実施の形態の構成例を示している。図１９に示す記録再生装置１９００は、図１に示すものとほぼ同様であるが、２つの記録媒体Ｉ／Ｆ１９０１、および１９０２を持ち、それぞれが記録媒体１９５１および１９５２と接続されるようになっている。

【０１０４】図２０に、図１９に示した記録再生装置を用いたコピーの処理フローを示す。この構成においては、実施例１で説明した図９のステップＳ９０１のような機器間での相互認証プロトコルは不要となっている。

【０１０５】ステップＳ２００１において、記録再生装置はコピー先となるメディア２のメディアＩＤを読出し、ステップＳ２００２では、コピーしてよいか否かの判断を行う。コピーの可否の判断は、先に図４を用いて説明したように、コピー履歴テーブル、この場合は、メディア１に格納されたコピー履歴テーブルにおいて、コ

ピー対象のコンテンツＩＤのデータに対応して設定されたコピー番号の欄１～Ｘに対応するコピー格納先メディアＩＤの欄に空欄がある場合にコピー可と判断する。

【０１０６】ステップＳ２００３およびＳ２００４は、図９のステップＳ９０４およびＳ９０５と同様であるので説明を省略する。

【０１０７】ステップＳ２００５では、メディア１からメディア２に対するコンテンツのコピーを実行する。このコンテンツコピー処理の詳細を図２１のフローに示す。

【０１０８】図２１の処理フローは、先に述べた他の処理フローと同様、特開平１１－２２４４６１号公報で提案した方式、すなわち複数の記録再生機器に共通に格納された秘密鍵（マスターキー）と記録媒体固有情報から暗号化キーおよび復号キーを生成する手法を適用した場合の処理フローである。

【０１０９】図２１のステップＳ２１０１乃至Ｓ２１０４は、先に説明した図１７のデバイスＡでの処理ステップＳ１７０２，Ｓ１７０３と、デバイスＢでの処理ステップＳ１７２２，Ｓ１７２３に相当するものであり、本実施例においては、同一機器内において、メディア１，２のＩＤを読み出して、それぞれのメディア用の暗号鍵（１）、（２）を生成する。

【０１１０】ステップＳ２１０５では、メディア１からコピーすべきコンテンツデータと、コピー履歴テーブルとを読み出して、ステップＳ２１０６において、先のステップＳ２１０２で生成した暗号鍵（暗号鍵(1)）を用いて、コンテンツデータと、コピー履歴テーブルとの復号処理を実行する。

【０１１１】ステップＳ２１０７において、デバイスは、復号したコピー履歴テーブルの編集処理を実行する。具体的には、図４に示すコピー履歴テーブルのコピー対象となるコンテンツのコピー格納先メディアＩＤ欄にメディア２のＩＤを書き込む。この書き込み処理の後、先に生成したデータ暗号鍵（暗号鍵(1)）を用いて編集後のコピー履歴テーブルを暗号化し、暗号化したコピー履歴テーブルをメディア１に記録する。

【０１１２】次に、ステップＳ２１０８において、デバイスは暗号鍵(2)を用いてコンテンツデータを暗号化し、ステップＳ２１０９において暗号化データをメディア２に記録する。

【０１１３】実施例２の構成では、図２０，２１の処理フローから理解されるように、図１７において２つの記録再生装置が行っていた処理を１つの記録再生装置が行うようになっているため、装置間でコンテンツデータを伝送する処理を省略できる。

【０１１４】［実施例３］以上の説明においては、コピー履歴テーブルの編集更新処理を行なうことにより、コピーの数を制限する構成について説明したが、従来例の欄で説明したＳＣＭＳ(Serial Copy Management Syste m)と組み合わせて、ネットワーク配信によるコンテンツ配信においてもコピーの数を制限することを可能とした構成について実施例３として説明する。これまでに規定されているＳＣＭＳには、何度でもコピーが許容されるコピーフリー（copy free）のデータであるか、１度だけコピーが許されている（copy once allowed）データであるか、またはコピーが禁止されている（copy prohibited）データであるか、これら３態様を表す信号が含まれる。上記３つの態様に加え、さらにコピー履歴テーブルによるコピー数を制限する場合を、コピー数制限ありとして設定する。このような設定をすることにより、インターネットを介したコンテンツ配信のようなネットワーク配信において、コンテンツプロバイダからの一次配信を受信した機器からの２次配信回数を制限することが可能となる。

【０１１５】例えばＳＣＭＳ信号として２ビット設定し、コピーフリー（copy free）の場合、［０，０］、１度だけコピーが許されている（copy once allowed）を［０，１］、コピー禁止（copy prohibited）を［０，１］とし、コピー履歴テーブルによるコピー数制限ありの場合を、［１，１］とする。これら４態様をＳＣＭＳ信号として設定してコピーの制限を行なう。ＳＣＭＳ信号が［１，１］、すなわち、コピー履歴テーブルによるコピー数制限ありの場合には、コピー数を設定するビットとしてコピー数設定ビットを数ビット、例えば４ビットを設定し、許可されたコピー数に応じて、コピー数設定ビットを設定する。例えば３回のみコピー可であれば［００１１］、５回コピー可であれば、［０１０１］等である。コンテンツプロバイダは、コンテンツの配信先にコンテンツとともに、これらのコピー数設定ビットを送信する。

【０１１６】コンテンツプロバイダからの一次配信を受信する機器において、コピー履歴テーブルによるコピー数制限ありの［１，１］の信号およびコピー数設定ビットを受信した場合、予め機器に格納されている、あるいは配信されるコピー履歴テーブル生成処理プログラムに従って、コピー数設定ビットに設定されたコピー数に応じたコピー履歴テーブルを生成する。生成したコピー履歴テーブルは、受信コンテンツとともに記録媒体に格納される。

【０１１７】生成するコピー履歴テーブルは、先に説明した図４と同様のものとなるが、コンテンツに対応して設定されるコピー番号は、コピー数設定ビットに設定された数、例えば、［００１１］であれば３、［０１０１］であれば５を上限とした数に設定される。なお、ＳＣＭＳ信号が［１，１］であり、コピー数設定ビットにコピー数の指定がない場合、もしくはコピー数設定ビットが伝送されない場合には、システムにあらかじめ定められているコピー数に対応したテーブルが作られる。すなわち、情報処理装置に予め設定済みのコピー許容回数

データ、例えばコピー数設定ビットの付与されないコンテンツに共通に適用するデータとして情報処理装置に設定されているコピー許容回数データに基づいてコピー履歴テーブルを生成して、生成したコピー制御テーブルに基づいてコピー制御処理を実行する。

【０１１８】このように、コピー制限数をコンテンツと併せて配信することにより、記録媒体から再生されてコピーされるコンテンツのみでなく、ネットワークを介して配信されるコンテンツに対してもコピー数の制限を行なうことが可能となる。

【０１１９】なお、コピー数設定ビットに基づいてコピー履歴テーブルを生成する構成に限らず、例えばコンテンツとともに、予め所定のコピー番号が設定されたコピー履歴テーブルを、コンテンツプロバイダが送信する構成としてもよい。また、予め所定のコピー番号が設定されたテーブル生成コマンドを送信して、受信側においてコマンドに応じたコピー履歴テーブルを生成する構成としてもよい。

【０１２０】［データ処理手段の構成］上述した一連の処理は、ハードウェアにより行うことは勿論、ソフトウェアにより行うこともできる。即ち、例えば、図１他で示す記録再生装置に構成される暗号処理手段１５０は暗号化／復号ＬＳＩとして構成することも可能であるが、汎用のコンピュータや、１チップのマイクロコンピュータにプログラムを実行させることにより行う構成とすることも可能である。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや１チップのマイクロコンピュータ等にインストールされる。図２２は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

【０１２１】プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク２２０５やＲＯＭ２２０３に予め記録しておくことができる。あるいは、プログラムはフロッピー（登録商標）ディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体２２１０に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体２２１０は、いわゆるパッケージソフトウエアとして提供することができる。

【０１２２】なお、プログラムは、上述したようなリムーバブル記録媒体２２１０からコンピュータにインストールする他、ダウンロードサイトから、ディジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、ＬＡＮ(Local AreaNetwork)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部２２０８で受信し、内蔵するハードディスク２２０５にインストールすることができる。

【０１２３】コンピュータは、ＣＰＵ(Central Processing Unit)２２０２を内蔵している。ＣＰＵ２２０２には、バス２２０１を介して、入出力インタフェース２２１１が接続されており、ＣＰＵ２２０２は、入出力インタフェース２２１０を介して、ユーザによって、キーボードやマウス等で構成される入力部２２０７が操作されることにより指令が入力されると、それにしたがって、ＲＯＭ(Read Only Memory)２２０３に格納されているプログラムを実行する。

【０１２４】あるいは、ＣＰＵ２２０２は、ハードディスク２２０５に格納されているプログラム、衛星若しくはネットワークから転送され、通信部２２０８で受信されてハードディスク２２０５にインストールされたプログラム、またはドライブ２２０９に装着されたリムーバブル記録媒体２２１０から読み出されてハードディスク２２０５にインストールされたプログラムを、ＲＡＭ(Random Access Memory)２２０４にロードして実行する。

【０１２５】これにより、ＣＰＵ２２０２は、上述したフローチャートにしたがった処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、ＣＰＵ２２０２は、その処理結果を、必要に応じて、例えば、入出力インタフェース２２１１を介して、ＬＣＤ(Liquid Crystal Display)やスピーカ等で構成される出力部２２０６から出力、あるいは、通信部２２０８から送信、さらには、ハードディスク２２０５に記録させる。

【０１２６】ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

【０１２７】また、プログラムは、１つのコンピュータにより処理されるものであっても良いし、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

【０１２８】なお、暗号化／復号処理は、１チップの暗号化／復号ＬＳＩで実行する構成、あるいはＣＰＵが実行する１つのソフトウェアモジュールとして実現することも可能である。

【０１２９】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０１３０】

【発明の効果】以上、説明したように、本発明の情報処理装置では、コピー数を設定したコピー履歴テーブルをコンテンツに対応付けて保有する構成としたので、データ（コンテンツ）ごとに作られるコピー（子）の数の制限が可能となる。具体的には、コンテンツデータごとにコピーの履歴テーブルを作成し、それに基づいてコピーを行うかどうか判定し、上限に達した以降のコピー処理を不可とする。すなわち、コピー実行の前に、コンテンツＩＤに対応して設定されたコピー格納先メディアＩＤ欄に、コピーを実行するメディアのメディアＩＤを書き込む処理を実行する構成としたので、予めコピー履歴テーブルのコピー番号として設定された数を超える場合は、メディアＩＤを書き込めず、コピーが実行されない。従って、テーブルに設定したコピーの数を超えるコピーが氾濫することを防止できる。

【０１３１】さらに、本発明の情報処理装置では、コピー制限数をコンテンツと併せて配信することにより、記録媒体から再生されてコピーされるコンテンツのみでなく、ネットワークを介して配信されるコンテンツに対してもコピー数の制限を行なうことが可能となる。

【図面の簡単な説明】

【図１】本発明の情報処理装置の構成例１を示すブロック図である。

【図２】本発明の情報処理装置の構成例２を示すブロック図である。

【図３】本発明の情報処理装置のコンテンツコピー時の接続態様例を示すブロック図である。

【図４】本発明の情報処理装置におけるコピー履歴テーブルの例を示す図である。

【図５】本発明の情報処理装置において使用可能な記録媒体の構成例（例１）を示す図である。

【図６】本発明の情報処理装置において使用可能な記録媒体の構成例（例２）を示す図である。

【図７】本発明の情報処理装置において使用可能な記録媒体の構成例（例３）を示す図である。

【図８】本発明の情報処理装置において使用可能な記録媒体の構成例（例４）を示す図である。

【図９】本発明の情報処理装置におけるコンテンツコピー処理フローを示す図である。

【図１０】本発明の情報処理装置において適用可能な認証処理（共通鍵方式）の処理シーケンスを示す図である。

【図１１】本発明の情報処理装置において適用可能な認証処理（公開鍵方式）の処理シーケンスを示す図である。

【図１２】本発明の情報処理装置において適用可能な認証処理に用いられる公開鍵証明書の構成を示す図である。

【図１３】本発明の情報処理装置におけるリポケーションリストの構成を示す図である。

【図１４】本発明の情報処理装置におけるレジストレーションリストの構成を示す図である。

【図１５】本発明の情報処理装置におけるコピー履歴テーブルを用いたコピー許可／不許可判定処理フローを示す図である。

【図１６】本発明の情報処理装置におけるコピー履歴テーブルの編集処理、格納処理フローを示す図である。

【図１７】本発明の情報処理装置におけるデバイス間でのコピー履歴テーブルを用いたコンテンツコピー処理フローを示す図である。

【図１８】本発明の情報処理装置のコンテンツコピー時の接続態様例を示すブロック図である。

【図１９】本発明の情報処理装置の実施例２における構成例を示すブロック図である。

【図２０】本発明の情報処理装置の実施例２におけるコンテンツコピー処理フローを示す図である。

【図２１】本発明の情報処理装置の実施例２におけるコンテンツコピー処理の詳細フローを示す図である。

【図２２】本発明の情報処理装置において、データ処理をソフトウェアによって実行する場合の処理手段構成を示したブロック図である。

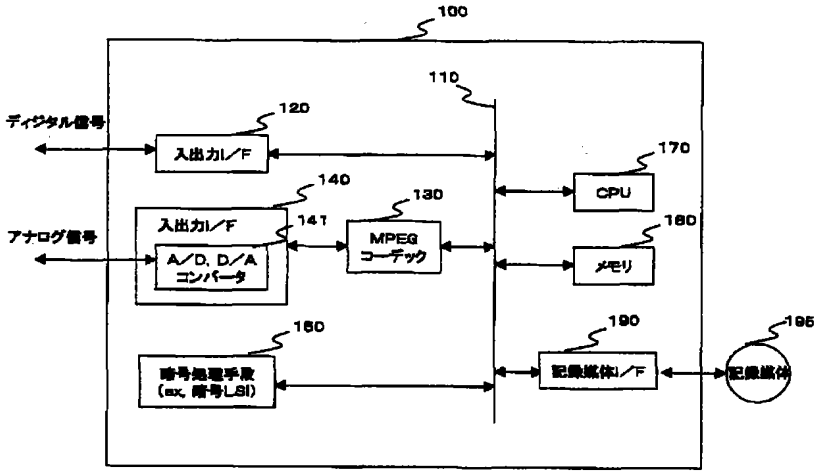
【符号の説明】

１００，２００　記録再生装置
１１０　バス
１２０　デジタルＩ／Ｆ
１３０　ＭＰＥＧコーデック
１４０　入出力Ｉ／Ｆ
１４５　Ａ／Ｄ．Ｄ／Ａコンバータ
１５０　暗号処理手段
１７０　ＣＰＵ
１８０　メモリ
１９０　記録媒体Ｉ／Ｆ
１９５　記録媒体
５０１　中心孔
５０２　ＲＡＭ領域
６０１　中心孔
６０２　ＲＡＭ領域
６０３　ＲＯＭ領域
７０１　カートリッジ
７０２　光ディスク
７０３　ＩＣチップ
８０１　カートリッジ
８０２　入出力端子
８０３　メモリコントロール用ＩＣチップ
８０４　ＩＣチップ
１９００　記録再生装置
１９０１，１９０２　記録媒体Ｉ／Ｆ
１９５１，１９５２　記録媒体
２２０１　バス
２２０２　ＣＰＵ

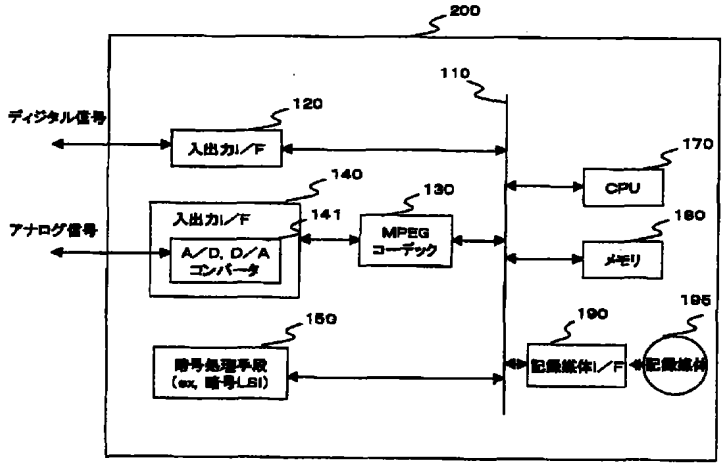
29　　30

２２０３　ＲＯＭ
２２０４　ＲＡＭ
２２０５　ハードディスク
２２０６　出力部
２２０７　入力部
＊２２０８　通信部
２２０９　ドライブ
２２１０　リムーバブル記録媒体
２２１１　入出力インタフェース
＊

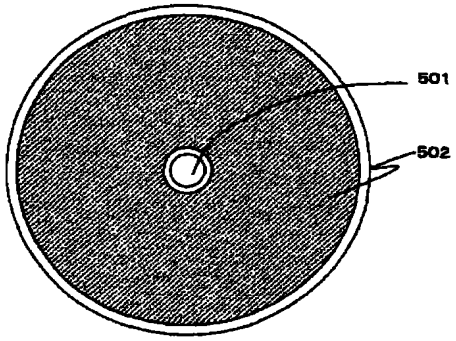
【図１】



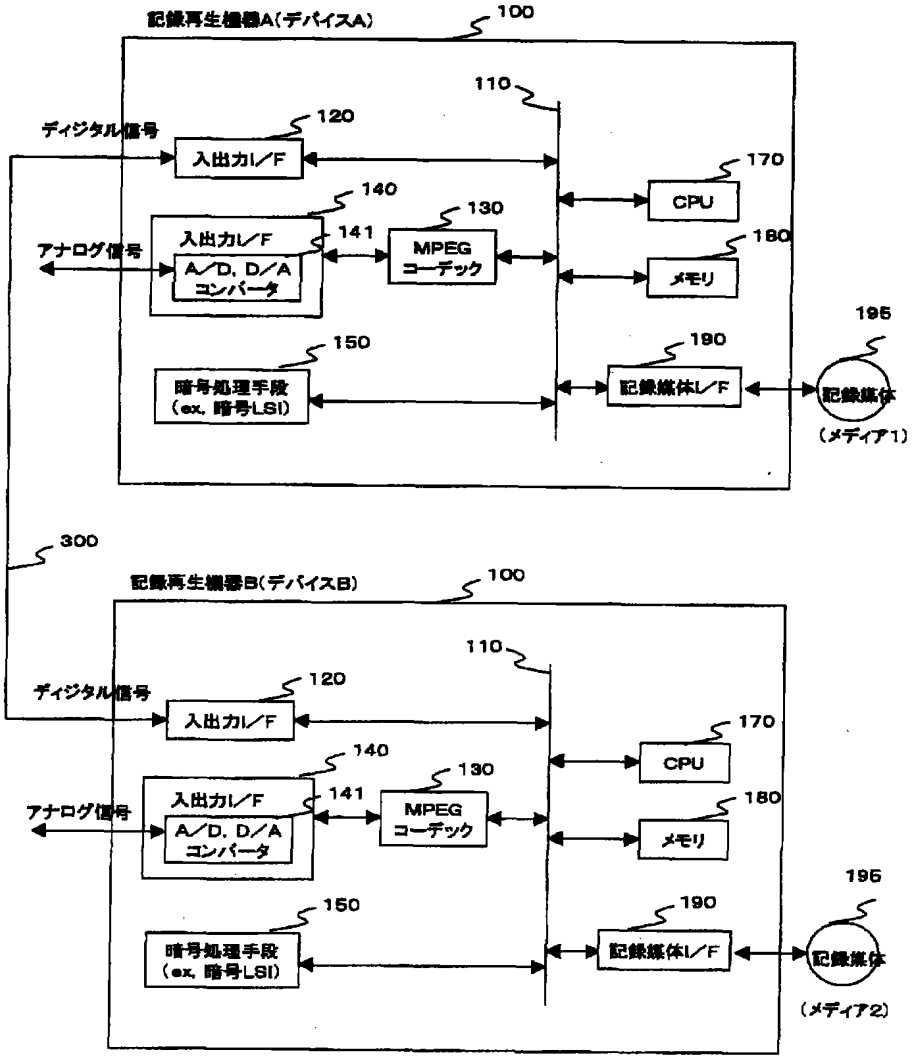
【図２】



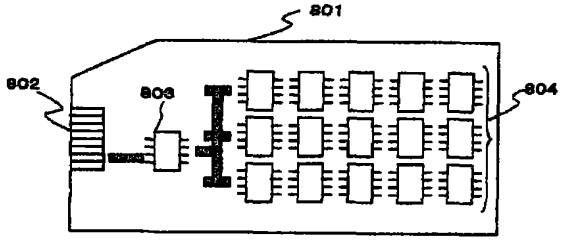
【図５】



【図３】



【図８】



【図１３】

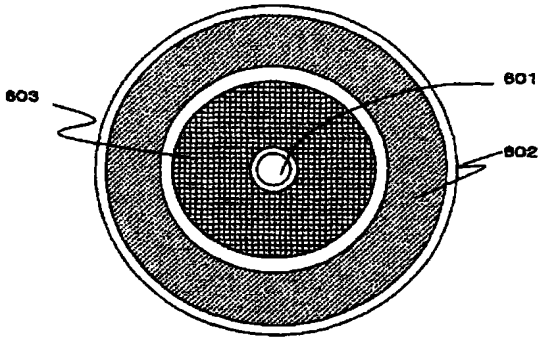
リボケーションリストのフォーマット

バージョンナンバ
リボークされる機器のID
:
センタのデジタル署名

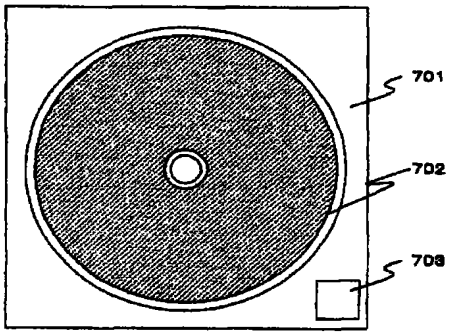
【図４】

コンテンツID	コピー番号	コピー格納先メディアID
12345678	1	abcdefgh
	2	87654321
	3	------
	...	------
	N	------
abcd1234	1	87654321
	2	------
	3	------
	...	------
	M	------
:	:	:

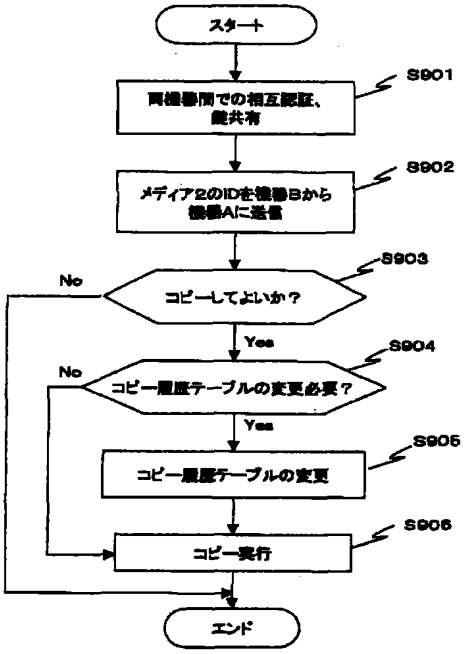
【図６】



【図７】



【図９】



【図１２】

デバイスAの公開鍵証明書(Cert_A)

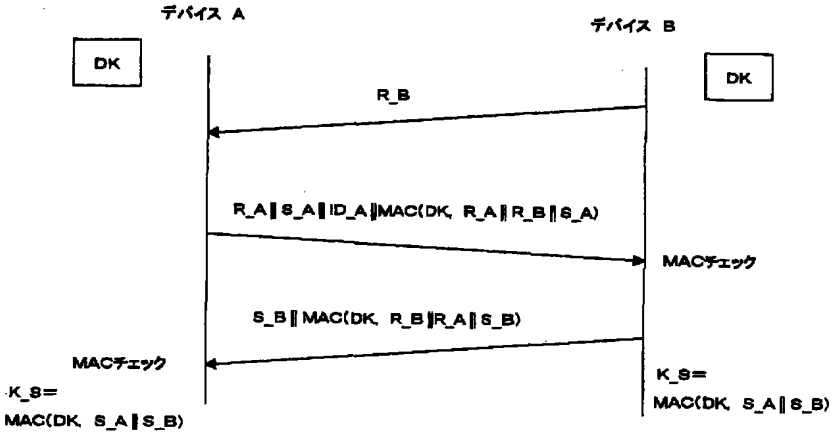
AのID(ID_A)
Aの公開鍵(Pubkey_A)
上記の全フィールドに対するセンタのデジタル署名

【図１４】

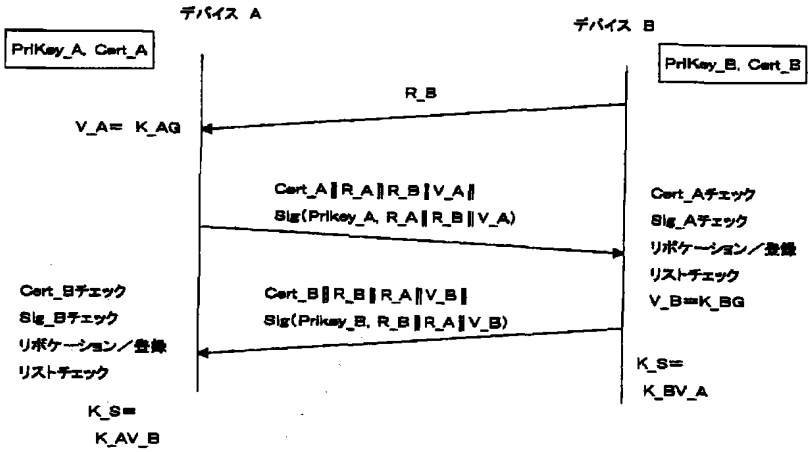
レジストレーションリストのフォーマット

バージョンナンバ
登録される機器のID
:
センタのデジタル署名

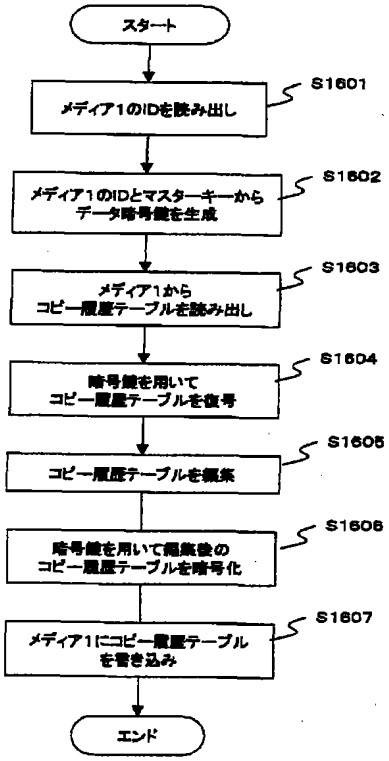
【図１０】


デバイス A
デバイス B
DK
DK
R_B
R_A‖S_A‖ID_A‖MAC(DK, R_A‖R_B‖S_A)
MACチェック
S_B‖MAC(DK, R_B‖R_A‖S_B)
MACチェック
K_S=
MAC(DK, S_A‖S_B)
K_S=
MAC(DK, S_A‖S_B)

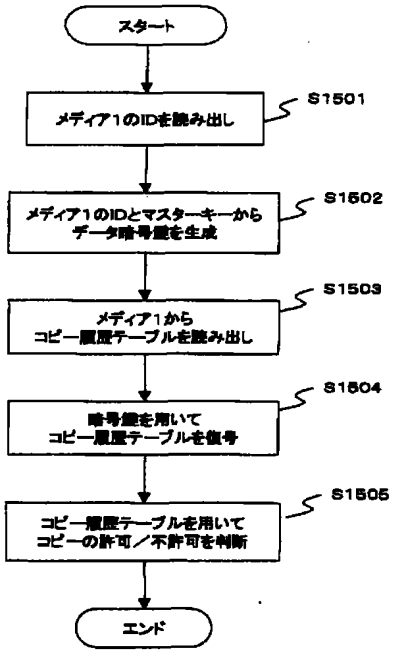
【図１１】


デバイス A
デバイス B
PriKey_A, Cert_A
PriKey_B, Cert_B
R_B
V_A= K_AG
Cert_A‖R_A‖R_B‖V_A‖
Sig(Prikey_A, R_A‖R_B‖V_A)
Cert_Aチェック
Sig_Aチェック
リボケーション／登録
リストチェック
V_B=K_BG
Cert_Bチェック
Sig_Bチェック
リボケーション／登録
リストチェック
Cert_B‖R_B‖R_A‖V_B‖
Sig(Prikey_B, R_B‖R_A‖V_B)
K_S=
K_BV_A
K_S=
K_AV_B

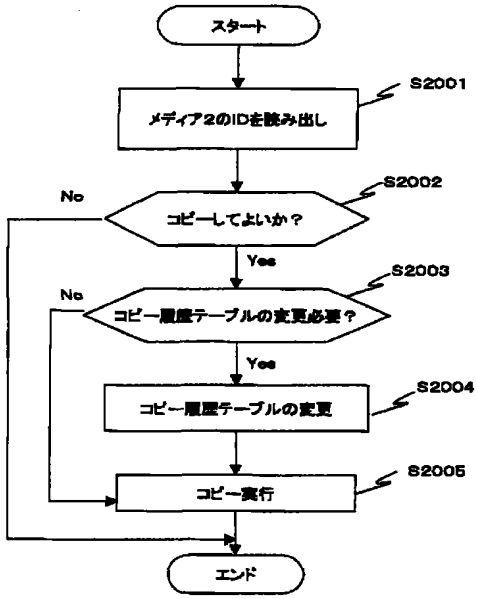
【図１６】


スタート
メディア1のIDを読み出し
S1601
メディア1のIDとマスターキーから
データ暗号鍵を生成
S1602
メディア1から
コピー履歴テーブルを読み出し
S1603
暗号鍵を用いて
コピー履歴テーブルを復号
S1604
コピー履歴テーブルを編集
S1605
暗号鍵を用いて編集後の
コピー履歴テーブルを暗号化
S1606
メディア1にコピー履歴テーブル
を書き込み
S1607
エンド

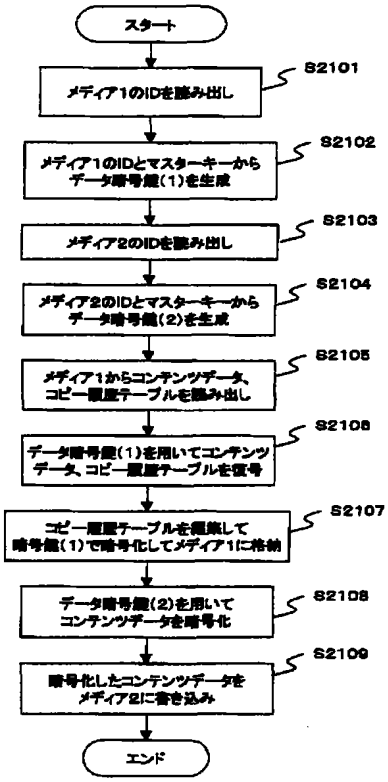
【図１５】


スタート
メディア1のIDを読み出し
S1501
メディア1のIDとマスターキーから
データ暗号鍵を生成
S1502
メディア1から
コピー履歴テーブルを読み出し
S1503
暗号鍵を用いて
コピー履歴テーブルを復号
S1504
コピー履歴テーブルを用いて
コピーの許可／不許可を判断
S1505
エンド

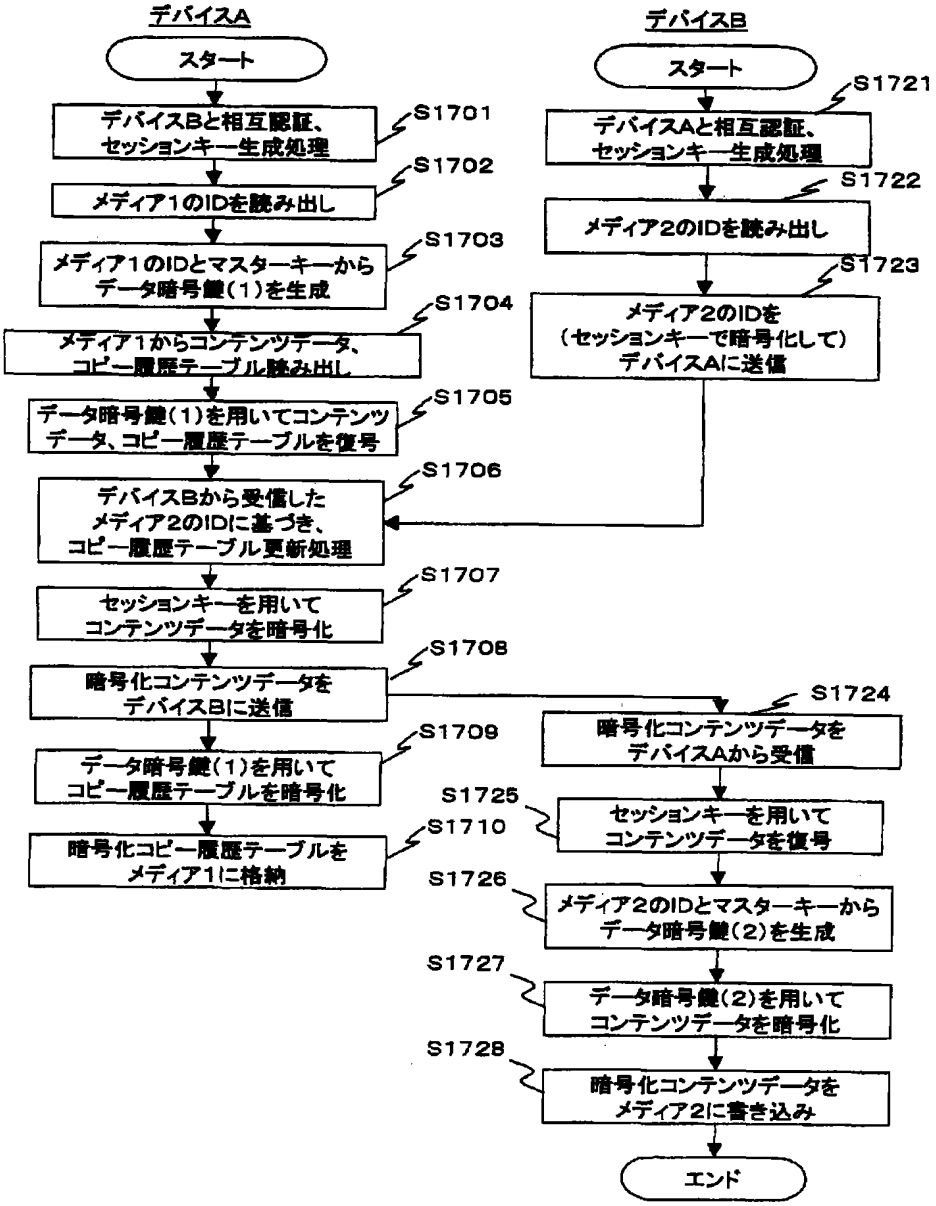
【図２０】


スタート
メディア2のIDを読み出し
S2001
No
コピーしてよいか？
S2002
Yes
No
コピー履歴テーブルの変更必要？
S2003
Yes
コピー履歴テーブルの変更
S2004
コピー実行
S2005
エンド

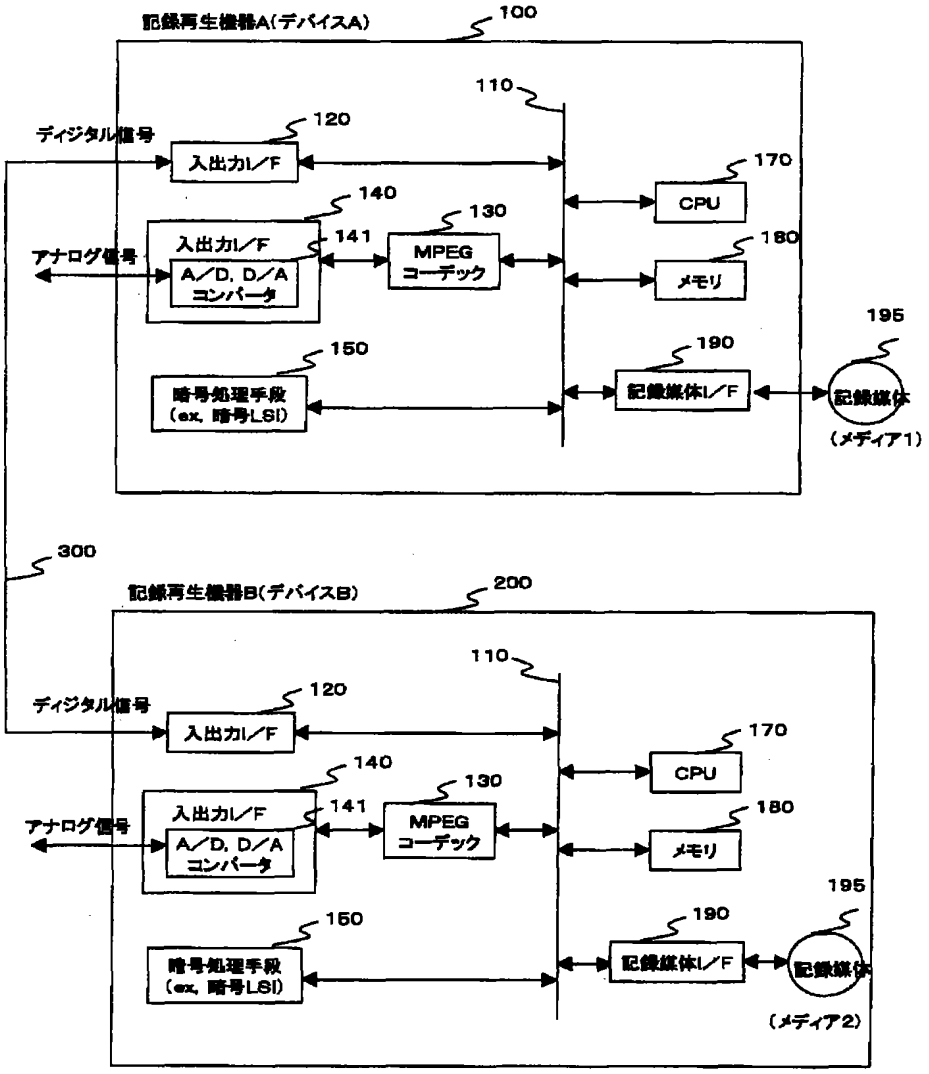
【図２１】


スタート
メディア1のIDを読み出し
S2101
メディア1のIDとマスターキーから
データ暗号鍵(1)を生成
S2102
メディア2のIDを読み出し
S2103
メディア2のIDとマスターキーから
データ暗号鍵(2)を生成
S2104
メディア1からコンテンツデータ、
コピー履歴テーブルを読み出し
S2105
データ暗号鍵(1)を用いてコンテンツ
データ、コピー履歴テーブルを復号
S2106
コピー履歴テーブルを編集して
暗号鍵(1)で暗号化してメディア1に格納
S2107
データ暗号鍵(2)を用いて
コンテンツデータを暗号化
S2108
暗号化したコンテンツデータを
メディア2に書き込み
S2109
エンド

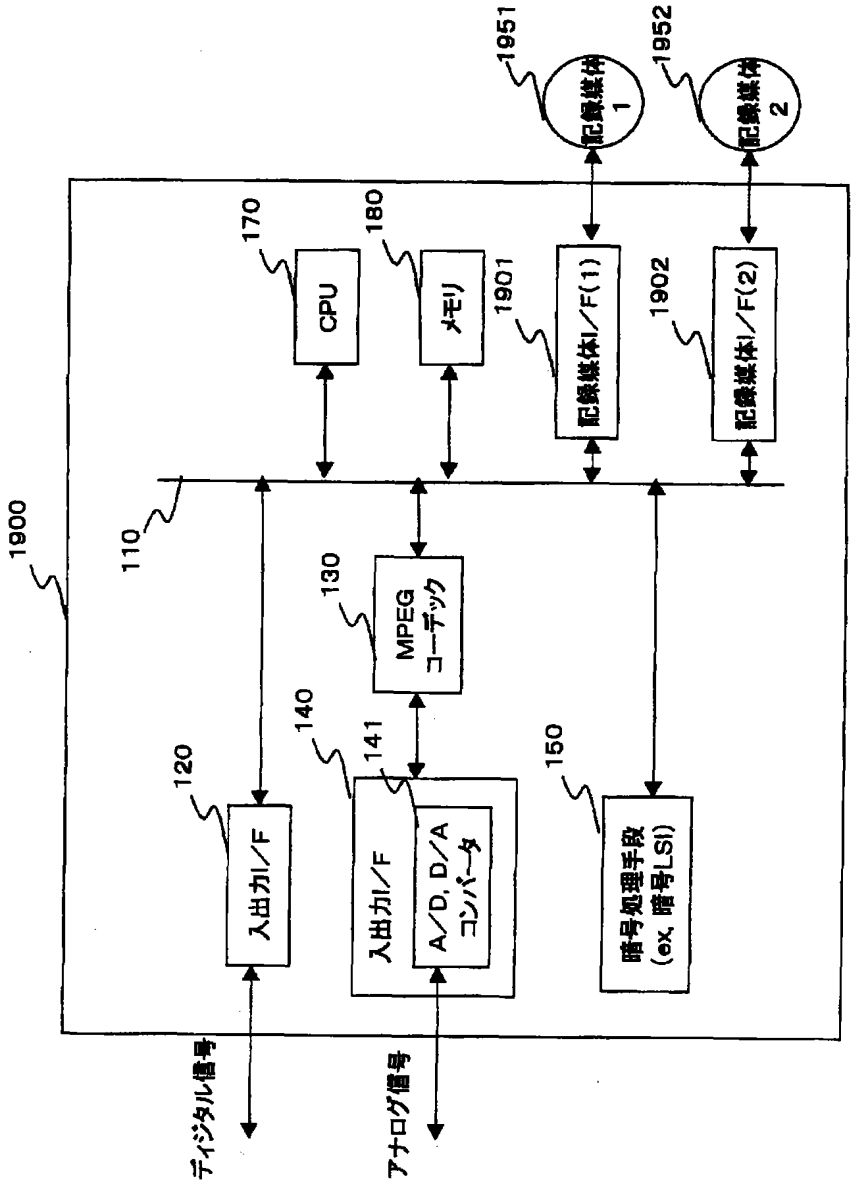
【図１７】


デバイスA
スタート
デバイスBと相互認証、セッションキー生成処理
S1701
メディア1のIDを読み出し
S1702
メディア1のIDとマスターキーからデータ暗号鍵(1)を生成
S1703
メディア1からコンテンツデータ、コピー履歴テーブル読み出し
S1704
データ暗号鍵(1)を用いてコンテンツデータ、コピー履歴テーブルを復号
S1705
デバイスBから受信したメディア2のIDに基づき、コピー履歴テーブル更新処理
S1706
セッションキーを用いてコンテンツデータを暗号化
S1707
暗号化コンテンツデータをデバイスBに送信
S1708
データ暗号鍵(1)を用いてコピー履歴テーブルを暗号化
S1709
暗号化コピー履歴テーブルをメディア1に格納
S1710
デバイスB
スタート
デバイスAと相互認証、セッションキー生成処理
S1721
メディア2のIDを読み出し
S1722
メディア2のIDを(セッションキーで暗号化して)デバイスAに送信
S1723
暗号化コンテンツデータをデバイスAから受信
S1724
セッションキーを用いてコンテンツデータを復号
S1725
メディア2のIDとマスターキーからデータ暗号鍵(2)を生成
S1726
データ暗号鍵(2)を用いてコンテンツデータを暗号化
S1727
暗号化コンテンツデータをメディア2に書き込み
S1728
エンド

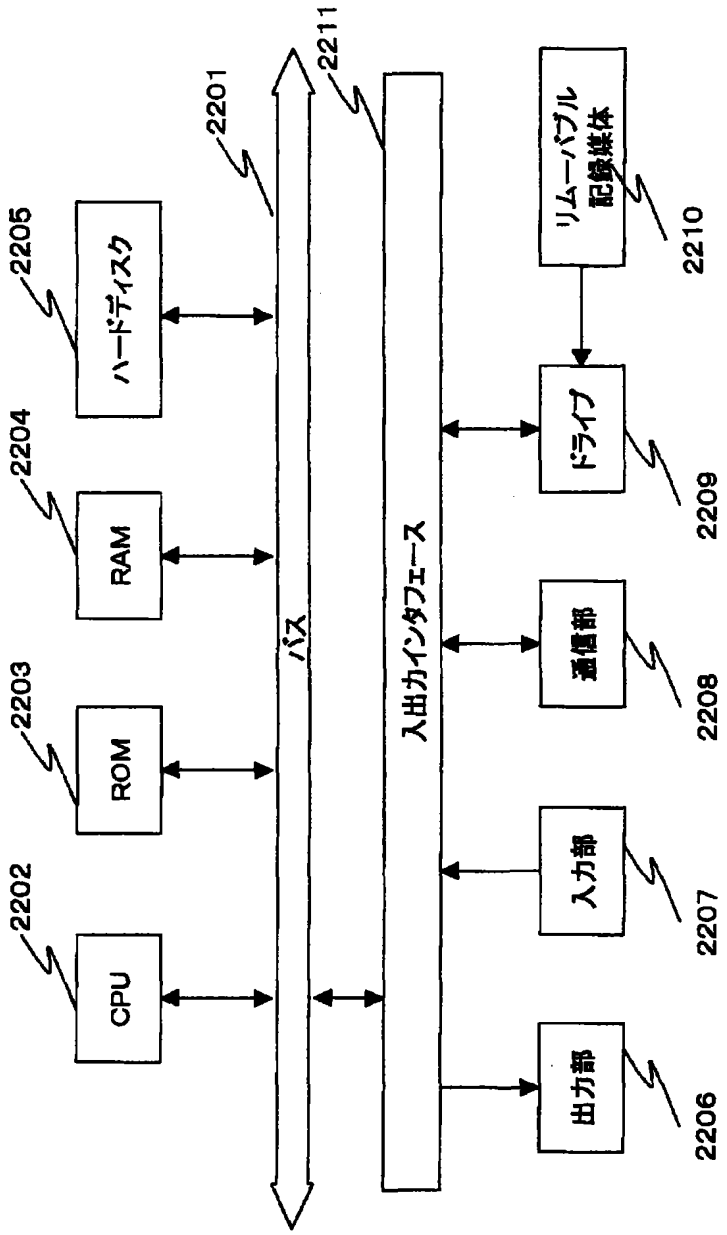
【図１８】


記録再生機器A(デバイスA)
100
110
ディジタル信号
120
入出力I／F
170
CPU
140
入出力I／F
141
A／D, D／A
コンバータ
130
MPEG
コーデック
アナログ信号
180
メモリ
195
150
暗号処理手段
(ex, 暗号LSI)
190
記録媒体I／F
記録媒体
(メディア1)
300
記録再生機器B(デバイスB)
200
110
ディジタル信号
120
入出力I／F
170
CPU
140
入出力I／F
141
A／D, D／A
コンバータ
130
MPEG
コーデック
アナログ信号
180
メモリ
195
150
暗号処理手段
(ex, 暗号LSI)
190
記録媒体I／F
記録媒体
(メディア2)

【図１９】


1951
記録媒体1
1952
記録媒体2
170
CPU
180
メモリ
1901
記録媒体I／F(1)
1902
記録媒体I／F(2)
1900
110
130
MPEGコーデック
140
141
120
入出力I／F
入出力I／F
A／D, D／Aコンバータ
150
暗号処理手段(ex, 暗号LSI)
ディジタル信号
アナログ信号

【図２２】



フロントページの続き

(51)Int.Cl.'	識別記号	FI	テーマコード（参考）
G06F 17/60	142	G06F 17/60	142

(72)発明者　中野　雄彦
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　北島　真理子
東京都品川区北品川６丁目７番35号　ソニー株式会社内

Ｆターム(参考)　5B017 AA06 BA07 BB10 CA15 CA16
5B049 AA05 BB00 CC00 DD05 FF09 GG04
5D044 AB05 BC04 CC04 DE17 DE50 GK17 HL08